

Multiple Access via Compute-and-Forward

Jingge Zhu and Michael Gastpar, *Member, IEEE*

Abstract

Lattice codes used under the Compute-and-Forward paradigm suggest an alternative strategy for the standard Gaussian multiple-access channel (MAC): The receiver successively decodes integer linear combinations of the messages until it can invert and recover all messages. In this paper, this strategy is developed and analyzed. For the two-user MAC, it is shown that without time-sharing, the entire capacity region can be attained with a single-user decoder as soon as the signal-to-noise ratios are above $1 + \sqrt{2}$. A partial analysis is given for more than two users. Lastly the strategy is extended to the so-called dirty MAC where two interfering signals are known non-causally to the two transmitters in a distributed fashion. Our scheme extends the previously known results and gives new achievable rate regions.

I. INTRODUCTION

Recent results on lattice codes applied to additive Gaussian networks show remarkable advantages of their linear structure. In particular the compute-and-forward scheme [1] demonstrates the idea that sometimes it is better to first decode sums of several codewords than the codewords individually. Similar ideas have also been exploited in several communication networks and are shown to be beneficial in various perspectives, see for example [2] [3] [4] [5].

The Gaussian multiple access channel is a well-understood communication system. To achieve its entire capacity region, the receiver can either use joint decoding (a multi-user decoder), or a single-user decoder combined with successive cancellation decoding and time-sharing [6, Ch. 15]. An extension of the successive cancellation decoding called Rate-Splitting Multiple Access is developed in [7] where only single-user decoders are used to achieve the whole capacity region without time-sharing, but at the price that messages have to be split to create more virtual users.

In this paper we provide and analyze a novel strategy for the Gaussian MAC using lattice codes based on a modified compute-and-forward technique. For the 2-user Gaussian MAC, the receiver first decodes the sum of the two transmitted codewords, and then decodes either one of the codewords, using the sum as side information. As an example, Figure 1 gives an illustration of an achievable rate region for a *symmetric* 2-user Gaussian MAC with our proposed scheme. When the *signal-to-noise ratio* (SNR) of both users is below 1.5, the proposed scheme cannot attain rate pairs on the dominant face of the capacity region. If the SNR exceeds 1.5, a line segment on the capacity boundary is achievable. As SNR increases, the end points of the line segment approach the corner points, and the whole capacity region is achievable as soon as the SNR of both users is larger than $1 + \sqrt{2}$. We point out that the decoder used in our scheme is a single-user decoder since it merely performs lattice quantizations on the received signal. Hence this novel approach allows us to achieve rate pairs in the capacity region using only a single-user decoder without time-sharing or rate splitting. This feature of the proposed coding scheme could be of interest for practical considerations.

The proposed coding scheme is then extended to the general K -user Gaussian MAC and achievable rate regions are derived. While a complete characterization of the achievable region is difficult to give for the general case, we raise a conjecture that the symmetric capacity¹ is always achievable for the symmetric Gaussian MAC, provided the

This work was supported in part by the European ERC Starting Grant 259530-ComCom. This paper was presented in part in Zurich International Seminar on Communications, Feb. 2014 and in part in IEEE International Symposium on Information Theory, Jun. 2014.

J. Zhu is with the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland (e-mail: jingge.zhu@epfl.ch).

M. Gastpar is with the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland and the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA (e-mail: michael.gastpar@epfl.ch).

¹For a symmetric K -user Gaussian MAC where the SNR of all users equals P , we say that the symmetric capacity is achievable if each user has a rate $\frac{1}{2K} \log(1 + KP)$.

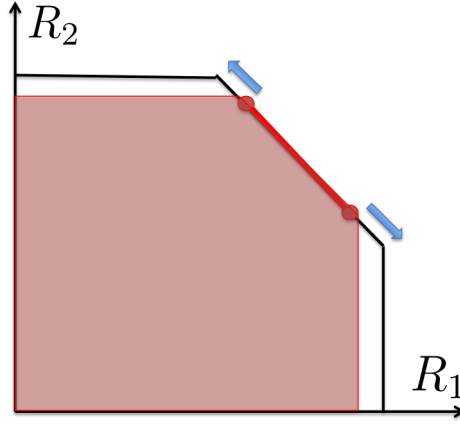


Fig. 1. An illustration of an achievable rate region for a 2-user Gaussian MAC with the proposed scheme. The rate pairs in the shaded region can be achieved using a single-user decoder without time-sharing. As SNR increases, the end points of the line segment approach the corner points and the whole capacity region becomes achievable. A sufficient condition for achieving the whole capacity region is that the SNR of both users are above $1 + \sqrt{2}$.

SNR exceeds a certain threshold. While this conjecture is established for the 2-user case where the SNR threshold is 1.5, some numerical evidence is given to support this conjecture for larger K . For example the numerical results suggest that the SNR threshold is less than 2.24 for the 3-user symmetric MAC and less than 3.75 for the 4-user symmetric MAC.

In a related result in [8] it is shown that under certain conditions, some isolated (non-corner) points of the capacity region can be attained. To prove this, the authors use fixed lattices which are independent of channel gains. From this perspective, our paper shows that if the lattices are properly scaled in accordance with the channel gains, then we can attain the full capacity region.

We then study the so-called “dirty” Gaussian MAC with two additive interference signals which are non-causally known to two encoders in a distributed manner. It was shown in [9] that lattice codes are well-suited for this problem. We devise a coding scheme within our framework to this system which extends the previous results and gives a new achievable rate region, which could be considerably larger for general interference strength.

Lastly we should point out that although this paper exclusively considers the Gaussian multiple access channel, the proposed coding scheme is more general and can be applied to many other Gaussian network problems.

The paper is organized as follows. Section II gives the problem statement and introduces the nested lattice codes used in our coding scheme. The important notion of computation rate tuple is also introduced. Section III gives a complete analysis of our coding scheme in the 2-user Gaussian MAC. In Section IV we extend the coding scheme to the K -user Gaussian MAC. A similar strategy is then applied to the Gaussian dirty MAC in Section V for the two user case.

Throughout this paper, vectors and matrices are denoted by lowercase and uppercase bold letters, such as \mathbf{a} and \mathbf{A} , respectively. The (i, j) -entry of a matrix \mathbf{A} is denoted by A_{ij} . The notation $\text{diag}(x_1, \dots, x_K)$ denotes a diagonal matrix whose diagonal entries are x_1, \dots, x_K . The determinant of a matrix \mathbf{A} is denoted by $|\mathbf{A}|$. The probability of a given event E is denoted by $\mathbb{P}(E)$.

II. NESTED LATTICE CODES AND COMPUTATION RATE TUPLES

We consider a K -user Gaussian multiple access channel. The discrete-time real Gaussian MAC has the following vector representation

$$\mathbf{y} = \sum_{k=1}^K h_k \mathbf{x}_k + \mathbf{z} \quad (1)$$

with $\mathbf{y}, \mathbf{x}_k \in \mathbb{R}^n$ denoting the channel output at the receiver and channel input of transmitter k . The Gaussian white noise with unit variance per entry is denoted by $\mathbf{z} \in \mathbb{R}^n$. A fixed real number h_k denotes the channel coefficient

from user k to the receiver and is known to transmitter k . We can assume without loss of generality that every user has the same power constraints on the channel input as $\mathbb{E}\{\|\mathbf{x}_k\|^2\} \leq nP$.

In our coding scheme, we map messages W_k of user k bijectively to points in \mathbb{R}^n denoted by \mathbf{t}_k , which are elements of the codebook \mathcal{C}_k to be defined later. The *rate* of the codebook \mathcal{C}_k is defined to be

$$r_k := \frac{1}{n} \log |\mathcal{C}_k| \quad \text{for } k = 1, 2 \quad (2)$$

Each transmitter is equipped with an encoder \mathcal{E}_k which maps its message (or the corresponding codeword) to the channel input as $\mathbf{x}_k = \mathcal{E}_k(\mathbf{t}_k)$. At the receiver, a decoder wishes to estimate all the messages using the channel output \mathbf{y} . The decoded codewords are denoted by $\hat{\mathbf{t}}_1, \dots, \hat{\mathbf{t}}_K$ and they are mapped back to messages. Hence we can define the message error probability as

$$P_{e,msg}^{(n)} := \mathbb{P}(\hat{\mathbf{t}}_k \neq \mathbf{t}_k, k = 1, \dots, K) \quad (3)$$

where n is the length of codewords.

We require the receiver to decode all messages from \mathbf{y} with arbitrarily small error. Formally we have the following definition.

Definition 1 (Message rate tuple): Consider a K -user Gaussian MAC in (1). We say a *message rate tuple* (R_1, \dots, R_K) is achievable if it holds that for any $\epsilon > 0$ there exists a number n , such that the message error probability in (3) satisfies $P_{e,msg}^{(n)} < \epsilon$ whenever the rate r_k defined in (2) of user k satisfies $r_k < R_k$ for $k = 1, \dots, K$.

The capacity region, equivalently all possible achievable message rate tuples, of a K -user Gaussian MAC is known, see for example [10], [11], [6, Ch. 15]. In this paper we devise a novel approach to achieve the capacity region of the Gaussian MAC.

A. Nested lattice codes

A lattice Λ is a discrete subgroup of \mathbb{R}^n with the property that if $\mathbf{t}_1, \mathbf{t}_2 \in \Lambda$, then $\mathbf{t}_1 + \mathbf{t}_2 \in \Lambda$. More details about lattices and lattice codes can be found in [12] [13]. Define the lattice quantizer $Q_\Lambda : \mathbb{R}^n \rightarrow \Lambda$ as

$$Q_\Lambda(\mathbf{x}) = \operatorname{argmin}_{\mathbf{t} \in \Lambda} \|\mathbf{t} - \mathbf{x}\|$$

and define the fundamental Voronoi region of the lattice to be

$$\mathcal{V} := \{\mathbf{x} \in \mathbb{R}^n : Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$$

The modulo operation gives the quantization error:

$$[\mathbf{x}] \bmod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x})$$

Two lattices Λ and Λ' are said to be nested if $\Lambda' \subseteq \Lambda$.

Let Λ be a simultaneously good lattice in the sense of [12] [13]. Let $\beta_k, k = 1, \dots, K$ be K nonzero real numbers and we collect them into one vector $\underline{\beta} := (\beta_1, \dots, \beta_K)$. We can construct lattices $\Lambda_k^s \subseteq \Lambda$ for all k where all lattices are simultaneously good and with second moment

$$\frac{1}{n \operatorname{Vol}(\mathcal{V}_k^s)} \int_{\mathcal{V}_k^s} \|\mathbf{x}\|^2 d\mathbf{x} = \beta_k^2 P$$

where \mathcal{V}_k^s denotes the Voronoi region of the lattice Λ_k^s . The lattice Λ_k^s is used as the *shaping region* for the codebook of user k .

For each transmitter k , we construct the codebook as

$$\mathcal{C}_k = \Lambda \cap \mathcal{V}_k^s \quad (4)$$

With this codebook the message rate of user k is

$$r_k = \frac{1}{n} \log |\mathcal{C}_k| = \frac{1}{n} \log \frac{\operatorname{Vol}(\mathcal{V}_k^s)}{\operatorname{Vol}(\mathcal{V})} \quad (5)$$

where \mathcal{V} is the Voronoi region of the fine lattice Λ .

The parameters $\underline{\beta}$ are used to control the individual rates of different users. We will see later that the proper choice of these parameters depend on the channel coefficients. We also note that a similar idea appears in [14] [15] whereas the authors do not make connections between these parameters and channel coefficients.

B. The computation rate tuple

Throughout this work, we will be interested in decoding integer sums of the lattice codewords of the form

$$\mathbf{u} := \sum_{k=1}^K a_k \mathbf{t}_k \quad (6)$$

where a_k is an integer. Let $\hat{\mathbf{u}}$ denote the decoded integer sum at the receiver and define the error probability of decoding a sum as

$$P_{e,sum}^{(n)} := \mathbb{P}(\hat{\mathbf{u}} \neq \mathbf{u}) \quad (7)$$

where n is the length of codewords. This idea is, in the first place, different from the usual decoding procedure where individual messages are decoded. To articulate the point, we give a definition of the computation rate tuple in the context of the K -user Gaussian MAC.

Definition 2 (Computation rate tuple): Consider a K -user Gaussian MAC in (1). We say a *computation rate tuple* $(R_1^{\mathbf{a}}, \dots, R_K^{\mathbf{a}})$ with respect to a sum with coefficients $\mathbf{a} := (a_1, \dots, a_K)$ is achievable if it holds for any $\epsilon > 0$ there exists a number n , such that the sum decoding error probability in (7) satisfies $P_{e,sum}^{(n)} < \epsilon$ whenever the rate r_k defined in (2) of user k satisfies $r_k < R_k^{\mathbf{a}}$ for $k = 1, \dots, K$.

An achievable computation rate tuple in the Gaussian MAC is given in the following theorem, as a generalization of the result of [1].

Theorem 1 (A general compute-and-forward formula): Consider a K -user Gaussian MAC with channel coefficients $\mathbf{h} = (h_1, \dots, h_K)$ and equal power constraint P . Let β_1, \dots, β_K be K nonzero real numbers. The computation rate tuple $(R_1^{\mathbf{a}}, \dots, R_K^{\mathbf{a}})$ with coefficients $\mathbf{a} =: (a_1, \dots, a_K)$ is achievable where

$$R_k^{\mathbf{a}} = \left[\frac{1}{2} \log \left(\|\tilde{\mathbf{a}}\|^2 - \frac{P(\mathbf{h}^T \tilde{\mathbf{a}})^2}{1 + P \|\mathbf{h}\|^2} \right)^{-1} + \frac{1}{2} \log \beta_k^2 \right]^+ \quad (8)$$

for all k where $\tilde{\mathbf{a}} := [\beta_1 a_1, \dots, \beta_K a_K]$ and $a_k \in \mathbb{Z}$ for all $k \in [1 : K]$.

Proof: A proof of this theorem is given in Appendix A. ■

Remark 1:

- By setting $\beta_k = 1$ for all k we recover the original compute-and-forward formula given in [1] Theorem 4.
- The usefulness of the parameters β_1, \dots, β_K lies in the fact that they can be chosen according to the channel coefficients h_k and power P . This is crucial to our coding scheme as we will see in the sequel.
- This formula also illustrates why it is without loss of generality to assume that all powers are equal. In the case that each transmitter has power P_k , just replace h_k by $h'_k := \sqrt{P_k/P} h_k$ for all k in (8).
- It is straightforward to extend the result when there are multiple receivers, see Theorem 2 in [16].
- Unlike most compute-and-forward coding schemes where a modulo integer sum (see [1, Def. 24]) is decoded, our scheme only considers decoding the integer sums $\sum_k a_k \mathbf{t}_k$ themselves. This approach suffices for our purpose and makes the presentation cleaner.

C. Message rate tuple vs. computation rate tuple

It is important to distinguish the achievable *message rate tuple* in Definition 1, where individual messages should be decoded, and the achievable *computation rate tuple* in Definition 2, where only one function of messages is to be decoded. The superscript \mathbf{a} in the notation $R_k^{\mathbf{a}}$ is used to emphasize the different decoding goals. We give an example of computation rate pairs for a 2-user Gaussian MAC in Figure 2. It is worth noting that the achievable computation rate region can be strictly larger than the achievable message rate region.

One simple yet important observation is that when the receiver has multiple sums, the two notions can be formally related in the following way.

Lemma 1 (Computation rate and message rate): Consider a K -user Gaussian MAC and let $\mathbf{a}_1, \dots, \mathbf{a}_K$ be K linearly independent K -length vectors. If all K computation rate tuples $(R_1^{\mathbf{a}_\ell}, \dots, R_K^{\mathbf{a}_\ell}), \ell = 1, \dots, K$ are achievable, then the message rate tuple (R_1, \dots, R_K) is achievable where

$$R_k = \min_{\ell} R_k^{\mathbf{a}_\ell} \quad (9)$$

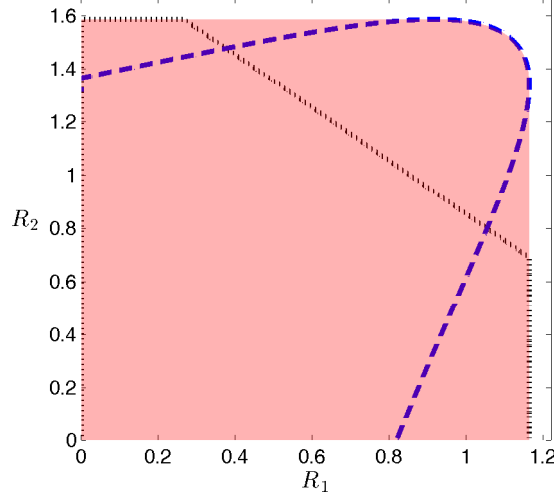


Fig. 2. In this figure we show an achievable computation rate region for computing the sum $\mathbf{t}_1 + \mathbf{t}_2$ over a 2-user Gaussian MAC where $h_1 = 1, h_2 = \sqrt{2}$ and $P = 4$. The dotted black line shows the capacity region of this MAC. The dashed blue line depicts the computation rate pairs given by (8) in Theorem 1. Points along this curve are obtained by choosing different β_1, β_2 . The shaded region shows the whole computation rate region, in which all the computation rate pairs are achievable. Notice that in this case the computation rate region contains the whole capacity region and is strictly larger than the latter.

for all $k = 1, \dots, K$.

Proof: Since $\mathbf{a}_1, \dots, \mathbf{a}_K$ are linearly independent vectors, the receiver can solve the individual codewords $\mathbf{t}_1, \dots, \mathbf{t}_K$ with such K sums. Also notice that in order to decode the sum with coefficient \mathbf{a}_ℓ , we need $r_k < R_k^{\mathbf{a}_\ell}$ for all $\ell = 1, \dots, K$. ■

III. THE 2-USER GAUSSIAN MAC

In this section we study the 2-user Gaussian MAC

$$\mathbf{y} = h_1 \mathbf{x}_1 + h_2 \mathbf{x}_2 + \mathbf{z} \quad (10)$$

with other specifications given in (1). We will give a complete characterization of the achievable rate region under our coding scheme.

The receiver decodes two integer sums of the two codewords as $\sum_{k=1}^2 a_k \mathbf{t}_k$ and $\sum_{k=1}^2 b_k \mathbf{t}_k$. We use \mathbf{a} to denote the row vector $(a_1, a_2) \in \mathbb{Z}^2$. Notice that if one sum, say $\sum_{k=1}^2 a_k \mathbf{t}_k$, is available at the decoder, it can be used along with the channel output \mathbf{y} to decode another sum. The following theorem gives achievable message rate pairs for the 2-user Gaussian MAC.

Theorem 2 (Achievable message rate pairs for the 2-user Gaussian MAC): Consider the 2-user multiple access channel in (10). The following message rate pair is achievable

$$R_k = \begin{cases} r_k(\mathbf{a}, \underline{\beta}) & \text{if } b_k = 0 \\ r_k(\mathbf{b}|\mathbf{a}, \underline{\beta}) & \text{if } a_k = 0 \\ \min\{r_k(\mathbf{a}, \underline{\beta}), r_k(\mathbf{b}|\mathbf{a}, \underline{\beta})\} & \text{otherwise} \end{cases}$$

for any linearly independent $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^2$ and $\underline{\beta} \in \mathbb{R}^2$ if it holds $r_k(\mathbf{a}, \underline{\beta}), r_k(\mathbf{b}|\mathbf{a}, \underline{\beta}) \geq 0$ for $k = 1, 2$, where we define

$$r_k(\mathbf{a}, \underline{\beta}) := \frac{1}{2} \log \frac{\beta_k^2 (1 + h_1^2 P + h_2^2 P)}{K(\mathbf{a}, \underline{\beta})} \quad (11)$$

$$r_k(\mathbf{b}|\mathbf{a}, \underline{\beta}) := \frac{1}{2} \log \frac{\beta_k^2 K(\mathbf{a}, \underline{\beta})}{\beta_1^2 \beta_2^2 (a_2 b_1 - a_1 b_2)^2} \quad (12)$$

with

$$K(\mathbf{a}, \underline{\beta}) := \sum_k a_k^2 \beta_k^2 + P(a_1 \beta_1 h_2 - a_2 \beta_2 h_1)^2 \quad (13)$$

Proof: The transmitted signal for user k is given by

$$\mathbf{x}_k = [\mathbf{t}_k / \beta_k + \mathbf{d}_k] \bmod \Lambda_k^s / \beta_k \quad (14)$$

where \mathbf{d}_k is called a *dither* which is a random vector uniformly distributed in the scaled Voronoi region $\mathcal{V}_k^s / \beta_k$. As pointed out in [12], \mathbf{x}_k is independent of \mathbf{t}_k and uniformly distributed in Λ_k^s / β_k hence has average power P_k for $k = 1, 2$.

Given two integers a_1, a_2 and some real number α_1 , we can form

$$\tilde{\mathbf{y}}_1 := \alpha_1 \mathbf{y} - \sum_k a_k \beta_k \mathbf{d}_k \quad (15)$$

$$= \underbrace{\sum_k (\alpha_1 h_k - a_k \beta_k) \mathbf{x}_k + \alpha_1 \mathbf{z}_1 + \sum_k a_k \beta_k \mathbf{x}_k - \sum_k a_k \beta_k \mathbf{d}_k}_{\tilde{\mathbf{z}}(1)} \quad (16)$$

$$\stackrel{(a)}{=} \tilde{\mathbf{z}}_1 + \sum_k a_k (\beta_k (\mathbf{t}_k / \beta_k + \mathbf{d}_k) - \beta_k Q_{\Lambda_k^s / \beta_k}(\mathbf{t}_k / \beta_k + \mathbf{d}_k)) - \sum_k a_k \beta_k \mathbf{d}_k \quad (17)$$

$$\stackrel{(b)}{=} \tilde{\mathbf{z}}_1 + \sum_k a_k (\mathbf{t}_k - Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k)) \quad (18)$$

$$= \tilde{\mathbf{z}}_1 + \sum_k a_k \tilde{\mathbf{t}}_k \quad (19)$$

with the notation

$$\tilde{\mathbf{z}}_1 := \sum_k (\alpha_1 h_k - \beta_k a_k) \mathbf{x}_k + \alpha_1 \mathbf{z} \quad (20)$$

$$\tilde{\mathbf{t}}_k := \mathbf{t}_k - Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k) \quad (21)$$

Step (a) follows from the definition of \mathbf{x}_k and step (b) uses the identity $Q_\Lambda(\beta \mathbf{x}) = \beta Q_{\Lambda/\beta}(\mathbf{x})$ for any real number $\beta \neq 0$. Note that $\tilde{\mathbf{t}}_k$ lies in Λ due to the nested construction $\Lambda_k^s \subseteq \Lambda$. The term $\tilde{\mathbf{z}}_1$ acts as an equivalent noise independent of $\sum_k a_k \tilde{\mathbf{t}}_k$ (thanks to the dithers) and has an average variance per dimension

$$N_1(\alpha_1) = \sum_k (\alpha_1 h_1 - \beta_k a_k)^2 P + \alpha_1^2 \quad (22)$$

The decoder obtains the sum $\sum_k a_k \tilde{\mathbf{t}}_k$ from $\tilde{\mathbf{y}}_1$ using *lattice decoding*: it quantizes $\tilde{\mathbf{y}}_1$ to its closest lattice point in Λ . Using the same argument in [1, Th. 5] [16, Th. 1], we can show this decoding process is successful if the rate of the transmitter k satisfies

$$r_k < r_k(\mathbf{a}, \underline{\beta}) = \max_{\alpha_1} \frac{1}{2} \log^+ \frac{\beta_k^2 P}{N_1(\alpha_1)} \quad (23)$$

Optimizing over α_1 we obtain the claimed expression in (11). In other words we have the computation rate pair $(R_1^{\mathbf{a}} := r_1(\mathbf{a}, \underline{\beta}), R_2^{\mathbf{a}} := r_2(\mathbf{a}, \underline{\beta}))$.² We remark that the expression (11) is exactly the general compute-and-forward formula given in Theorem 1 for $K = 2$.

²Strictly speaking, the computation rate pair is defined under the condition that the sum $\sum_k a_k \mathbf{t}_k$ can be decoded in Definition 2. Here we actually decode the sum $\sum_k a_k \tilde{\mathbf{t}}_k$. However this will not affect the achievable message rate pair, because we can also recover the two messages \mathbf{t}_1 and \mathbf{t}_2 using the two sums $\sum_k a_k \tilde{\mathbf{t}}_k$ and $\sum_k b_k \tilde{\mathbf{t}}_k$, as shown in the proof.

To decode a second integer sum with coefficients \mathbf{b} we use the idea of successive cancellation [1][17]. If $r_k(\mathbf{a}, \underline{\beta}) > 0$ for $k = 1, 2$, i.e., the sum $\sum_k a_k \tilde{\mathbf{t}}_k$ can be decoded, we can reconstruct the term $\sum_k a_k \beta_k \mathbf{x}_k$ as $\sum_k a_k \beta_k \mathbf{x}_k = \sum_k a_k \tilde{\mathbf{t}}_k + \sum_k a_k \beta_k \mathbf{d}_k$. Similar to the derivation of (19), we can use $\sum_k a_k \beta_k \mathbf{x}_k$ to form

$$\tilde{\mathbf{y}}_2 := \alpha_2 \mathbf{y} + \lambda \left(\sum_k a_k \beta_k \mathbf{x}_k \right) - \sum_k b_k \beta_k \mathbf{d}_k \quad (24)$$

$$= \sum_k (\alpha_2 h_k - (b_k + \lambda a_k) \beta_k) \mathbf{x}_k + \alpha_2 \mathbf{z} + \sum_k b_k \tilde{\mathbf{t}}_k \quad (25)$$

$$= \tilde{\mathbf{z}}_2 + \sum_k b_k \tilde{\mathbf{t}}_k \quad (26)$$

where the equivalent noise

$$\tilde{\mathbf{z}}_2 := \sum_k (\alpha_2 h_k - (b_k + \lambda a_k) \beta_k) \mathbf{x}_k + \alpha_2 \mathbf{z} \quad (27)$$

has average power per dimension

$$N_2(\alpha_2, \lambda) = \sum_k (\alpha_2 h_k - (b_k + \lambda a_k) \beta_k)^2 P + \alpha_2^2. \quad (28)$$

Under lattice decoding, the term $\sum_k b_k \tilde{\mathbf{t}}_k$ can be decoded if for $k = 1, 2$ we have

$$r_k < r_k(\mathbf{b}|\mathbf{a}, \underline{\beta}) = \max_{\alpha_2, \lambda} \frac{1}{2} \log^+ \frac{\beta_k^2 P}{N_2(\alpha_2, \lambda)} \quad (29)$$

Optimizing over α_2 and λ gives the claimed expression in (12). In other words we have the computation rate pair $(R_1^{\mathbf{b}} := r_1(\mathbf{b}|\mathbf{a}, \underline{\beta}), R_2^{\mathbf{b}} := r_2(\mathbf{b}|\mathbf{a}, \underline{\beta}))$.

With Lemma 1 and the fact that two vectors \mathbf{a} and \mathbf{b} are linearly independent, we know that a message pair (R_1, R_2) is achievable with

$$R_k = \min\{r_k(\mathbf{a}, \underline{\beta}), r_k(\mathbf{b}|\mathbf{a}, \underline{\beta})\} \quad (30)$$

An important observation is that when we decode a sum $\sum_k a_k \tilde{\mathbf{t}}_k$ with the coefficient $a_i = 0$, the lattice point $\tilde{\mathbf{t}}_i$ does not participate in the sum $\sum_k a_k \tilde{\mathbf{t}}_k$ hence the rate R_i will not be constrained by this decoding procedure as in (23). For example if we decode $a_1 \tilde{\mathbf{t}}_1 + a_2 \tilde{\mathbf{t}}_2$ with $a_1 = 0$, the computation rate pair is actually $(R_1^{\mathbf{a}} = \infty, R_2^{\mathbf{a}} = r_1(\mathbf{a}, \underline{\beta}))$, since the rate of user 1 in this case can be arbitrarily large. The same argument holds for the case $b_k = 0$. Combining (30) and the special cases when a_k or b_k equals zero, we have the claimed result. ■

Now we state the main theorem in this section showing it is possible to use the above scheme to achieve non-trivial rate pairs satisfying $R_1 + R_2 = C_{\text{sum}} := \frac{1}{2} \log(1 + h_1^2 P + h_2^2 P)$. Furthermore, we show that the whole capacity region is achievable under certain conditions on h_1, h_2 and P .

Theorem 3 (Capacity achieving for the 2-user Gaussian MAC): We consider the two-user Gaussian MAC in (10) where two sums with coefficients \mathbf{a} and \mathbf{b} are decoded. We assume that $a_k \neq 0$ for $k = 1, 2$ and define

$$A := \frac{h_1 h_2 P}{\sqrt{1 + h_1^2 P + h_2^2 P}}. \quad (31)$$

Case I): If it holds that

$$A < 3/4, \quad (32)$$

the sum capacity cannot be achieved by the proposed coding scheme.

Case II): If it holds that

$$A \geq 3/4, \quad (33)$$

the sum rate capacity can be achieved by decoding two integer sums using $\mathbf{a} = (1, 1), \mathbf{b} = (0, 1)$ with message rate pairs

$$R_1 = r_1(\mathbf{a}, \beta_2), R_2 = r_2(\mathbf{b}|\mathbf{a}, \beta_2), \text{ with } \beta_2 \in [\beta_2', \beta_2''] \quad (34)$$

or using $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 0)$ with message rate pairs

$$R_1 = r_1(\mathbf{b}|\mathbf{a}, \beta_2), R_2 = r_2(\mathbf{a}, \beta_2), \text{ with } \beta_2 \in [\beta'_2, \beta''_2] \quad (35)$$

where β'_2, β''_2 are two real roots of the quadratic equation

$$f(\beta_2) := K(\mathbf{a}, \beta_2) - \beta_2 \sqrt{1 + h_1^2 P + h_2^2 P} = 0 \quad (36)$$

The expressions $r_k(\mathbf{a}, \beta_2)$, $r_k(\mathbf{b}|\mathbf{a}, \beta_2)$ and $K(\mathbf{a}, \beta_2)$ are given in (11), (12) and (13) by setting $\beta_1 = 1$, respectively.

Case III: If it holds that

$$A \geq 1, \quad (37)$$

by choosing $\mathbf{a} = (1, 1)$ and $\mathbf{b} = (0, 1)$ or $\mathbf{b} = (1, 0)$, the achievable rate pairs in (34) and (35) cover the whole dominant face of the capacity region.

Proof: It is easy to see from the rate expressions (11) and (12) that we can without loss of generality assume $\beta_1 = 1$ in the following derivations. We do not consider the case when $a_k = 0$ for $k = 1$ or $k = 2$, which is just the classical interference cancellation decoding. Also notice that it holds:

$$r_1(\mathbf{a}, \beta_2) + r_2(\mathbf{b}|\mathbf{a}, \beta_2) = r_2(\mathbf{a}, \beta_2) + r_1(\mathbf{b}|\mathbf{a}, \beta_2) = \frac{1}{2} \log \frac{1 + (h_1^2 + h_2^2)P}{(a_2 b_1 - a_1 b_2)^2} = C_{sum} - \log |a_2 b_1 - a_1 b_2| \quad (38)$$

We start with **Case I** when the sum capacity cannot be achieved. This happens when

$$r_k(\mathbf{a}, \beta_2) < r_k(\mathbf{b}|\mathbf{a}, \beta_2), k = 1, 2 \quad (39)$$

for any choice of β_2 , which is equivalent to

$$f(\beta_2) > 0 \quad (40)$$

where $f(\beta_2)$ is given in (36). To see this, notice that Theorem 2 implies that in this case the sum message rate is

$$R_1 + R_2 = r_1(\mathbf{a}, \beta_2) + r_2(\mathbf{a}, \beta_2) \quad (41)$$

for $a_k \neq 0$. Due to Eqn. (38) we can upper bound the sum message rate by

$$R_1 + R_2 < r_1(\mathbf{a}) + r_2(\mathbf{b}|\mathbf{a}, \beta_2) \leq C_{sum} \quad (42)$$

$$R_1 + R_2 < r_2(\mathbf{a}) + r_1(\mathbf{b}|\mathbf{a}, \beta_2) \leq C_{sum}, \quad (43)$$

meaning the sum capacity is not achievable. It remains to characterize the condition under which the inequality $f(\beta_2) > 0$ holds. It is easy to see the expression $f(\beta_2)$ is a quadratic function of β_2 with the leading coefficient $a_2^2(1 + h_1^2 P)$. Hence $f(\beta_2) > 0$ always holds if the equation $f(\beta_2) = 0$ does not have any real root. The solutions of $f(\beta_2) = 0$ are given by

$$\beta'_2 := \frac{2a_1 a_2 h_1 h_2 P + S - \sqrt{SD}}{2(a_2^2 + a_2^2 h_1^2 P)} \quad (44a)$$

$$\beta''_2 := \frac{2a_1 a_2 h_1 h_2 P + S + \sqrt{SD}}{2(a_2^2 + a_2^2 h_1^2 P)} \quad (44b)$$

with

$$S := \sqrt{1 + (h_1^2 + h_2^2)P} \quad (45)$$

$$D := S(1 - 4a_1^2 a_2^2) + 4P a_1 a_2 h_1 h_2 \quad (46)$$

Inequality $f(\beta_2) > 0$ holds for all real β_2 if $D < 0$ or equivalently

$$\frac{h_1 h_2 P}{\sqrt{1 + (h_1^2 + h_2^2)P}} < \frac{4a_1^2 a_2^2 - 1}{4a_1 a_2} \quad (47)$$

The R.H.S. of the above inequality is minimized by choosing $a_1 = a_2 = 1$ which yields the condition (32). This is shown in Figure 3a: in this case the computation rate pair of the first sum $\tilde{\mathbf{t}}_1 + \tilde{\mathbf{t}}_2$ is too small and it cannot reach the sum capacity.

In **Case II** we require $r_k(\mathbf{a}, \beta_2) \geq r_k(\mathbf{b}|\mathbf{a}, \beta_2)$ or equivalently $f(\beta_2) \leq 0$ for some β_2 . By the derivation above, this is possible if $D \geq 0$ or equivalently

$$\frac{h_1 h_2 P}{\sqrt{1 + (h_1^2 + h_2^2)P}} \geq \frac{4a_1^2 a_2^2 - 1}{4a_1 a_2} \quad (48)$$

If we choose the coefficients to be $\mathbf{a} = (a_1, a_2)$ and $\mathbf{b} = (0, b_2)$ for some nonzero integers a_1, a_2, b_2 , Theorem 2 implies the sum rate is

$$R_1 + R_2 = r_1(\mathbf{a}, \beta_2) + r_2(\mathbf{b}|\mathbf{a}, \beta_2) = C_{\text{sum}} - \log |a_2 b_1 - a_1 b_2| \quad (49)$$

If the coefficients satisfy $|a_2 b_1 - a_1 b_2| = 1$, the sum capacity is achievable by choosing $\beta_2 \in [\beta_2', \beta_2'']$, with which the inequality (48) holds. Notice that if we choose $\beta_2 \notin [\beta_2', \beta_2'']$, then $r_k(\mathbf{a}, \beta_2) < r_k(\mathbf{b}|\mathbf{a}, \beta_2)$ and we are back to Case I). The condition $|a_2 b_1 - a_1 b_2| = 1$ is satisfied if the coefficients are chosen to be $\mathbf{a} = (1, 1)$, $\mathbf{b} = (0, 1)$. For simplicity we collect these two vectors and denote them as $\mathbf{A}_1 := (\mathbf{a}^T, \mathbf{b}^T)^T$.

The same result holds if the coefficients are of the form $\mathbf{a} = (a_1, a_2)$, $\mathbf{b} = (b_1, 0)$ and in particular $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 0)$. Similarly we denote these two vectors using $\mathbf{A}_2 := (\mathbf{a}^T, \mathbf{b}^T)^T$. We will let the coefficients be \mathbf{A}_1 or \mathbf{A}_2 for now and comment on other choices of coefficients later. With this choice of \mathbf{a} the inequality (48) is just the condition (33).

In general, not the whole dominant face of the capacity region can be achieved by varying $\beta_2 \in [\beta_2', \beta_2'']$. One important choice of β_2 is $\beta_2^{(1)} := \frac{h_1 h_2 P}{1 + h_1^2 P}$. With this choice of β_2 and coefficients \mathbf{A}_1 we have

$$R_1 = r_1(\mathbf{a}, \beta_2^{(1)}) = \frac{1}{2} \log(1 + h_1^2 P) \quad (50)$$

$$R_2 = r_2(\mathbf{b}|\mathbf{a}, \beta_2^{(1)}) = \frac{1}{2} \log\left(1 + \frac{h_2^2 P}{1 + h_1^2 P}\right) \quad (51)$$

which is one corner point of the capacity region. Similarly with $\beta_2^{(2)} := \frac{1 + h_2^2 P}{h_1 h_2 P}$ and coefficients \mathbf{A}_2 we have

$$R_2 = r_2(\mathbf{a}, \beta_2^{(2)}) = \frac{1}{2} \log(1 + h_2^2 P) \quad (52)$$

$$R_1 = r_1(\mathbf{b}|\mathbf{a}, \beta_2^{(2)}) = \frac{1}{2} \log\left(1 + \frac{h_1^2 P}{1 + h_2^2 P}\right) \quad (53)$$

which is another corner point of the capacity region. If the condition $\beta_2^{(1)}, \beta_2^{(2)} \notin [\beta_2', \beta_2'']$ is not fulfilled, we cannot choose β_2 to be $\beta_2^{(1)}$ or $\beta_2^{(2)}$ hence cannot achieve the corner points of the capacity region. In Figure 3b we give an example in this case where only part of rate pairs on the dominant face can be achieved.

In **Case III** we require $\beta_2^{(1)}, \beta_2^{(2)} \in [\beta_2', \beta_2'']$. In Appendix B we show that $\beta_2^{(1)}, \beta_2^{(2)} \in [\beta_2', \beta_2'']$ if and only if the condition (37) is satisfied. With the coefficients \mathbf{A}_1 , the achievable rate pairs $(r_1(\mathbf{a}, \beta_2), r_2(\mathbf{b}|\mathbf{a}, \beta_2))$ lies on the dominant face by varying β_2 in the interval $[\beta_2', \beta_2^{(1)}]$ and in this case we do not need to choose β_2 in the interval $(\beta_2^{(1)}, \beta_2'']$, see Figure 4a for an example. Similarly with coefficients \mathbf{A}_2 , the achievable rate pairs $(r_1(\mathbf{b}|\mathbf{a}, \beta_2), r_2(\mathbf{a}, \beta_2))$ lie on the dominant face by varying β_2 in the interval $[\beta_2^{(2)}, \beta_2'']$ and we do not need to let β_2 take values in the interval $[\beta_2', \beta_2^{(2)})$, see Figure 4b for an example. Since we always have $r_1(\mathbf{a}, \beta_2') \leq r_1(\mathbf{b}|\mathbf{a}, \beta_2'')$ and $r_2(\mathbf{b}|\mathbf{a}, \beta_2') \geq r_2(\mathbf{a}, \beta_2'')$, the achievable rate pairs with coefficients \mathbf{A}_1 and \mathbf{A}_2 cover the whole dominant face of the capacity region. ■

Remark 2: For any h_1, h_2 and P , applying Theorem 2 to two trivial sums with coefficients $\mathbf{a} = (1, 0)$, $\mathbf{b} = (0, 1)$ or $\mathbf{a} = (0, 1)$, $\mathbf{b} = (1, 0)$ allows us to obtain the corner points of the capacity region. In this case the proposed scheme reduces to the well-known successive cancellation decoding.

Remark 3: Notice that the decoder used for lattice decoding is in fact a single-user decoder since it only requires performing lattice quantizations on the received signal. Figure 5 shows the achievability of our scheme for different values of received signal-to-noise ratio $h_k^2 P$. In Region III (a sufficient condition is $h_k^2 P \geq 1 + \sqrt{2}$ for $k = 1, 2$), we can achieve any point in the capacity region using only a single-user decoder without time-sharing or rate splitting.

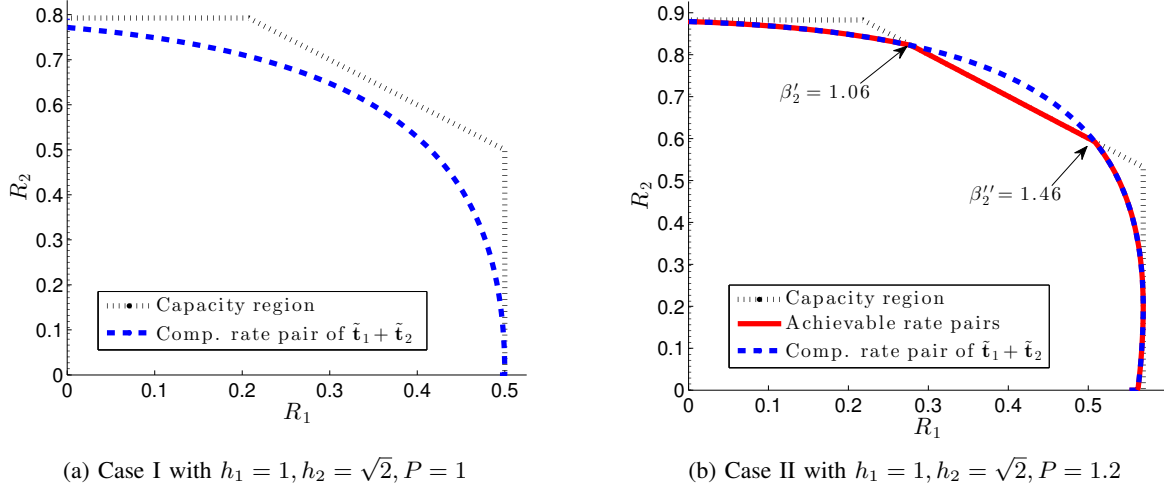


Fig. 3. Plot (a) shows the achievable rate pairs in Case I. In this case the condition (32) is satisfied and the computation rate pair of the first sum is too small. It has no intersection with the dominant face hence cannot achieve sum rate capacity. Notice that the (message) rate pairs contained in the computation rate region are achievable. Plot (b) shows the situation in Case II. In this case the condition (33) is fulfilled and the computation rate pair of the first sum is larger. It intersects with the dominant face, hence the sum capacity is achievable. In this example the condition (37) is not satisfied hence only part of the dominant face can be achieved, as depicted in the plot. The rate pair segment on the dominant face can be achieved by choosing $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 0)$ or $\mathbf{b} = (0, 1)$ and varying $\beta_2 \in [\beta'_2, \beta''_2]$. Choosing β_2 to be β'_2, β''_2 gives the end points of the segment.

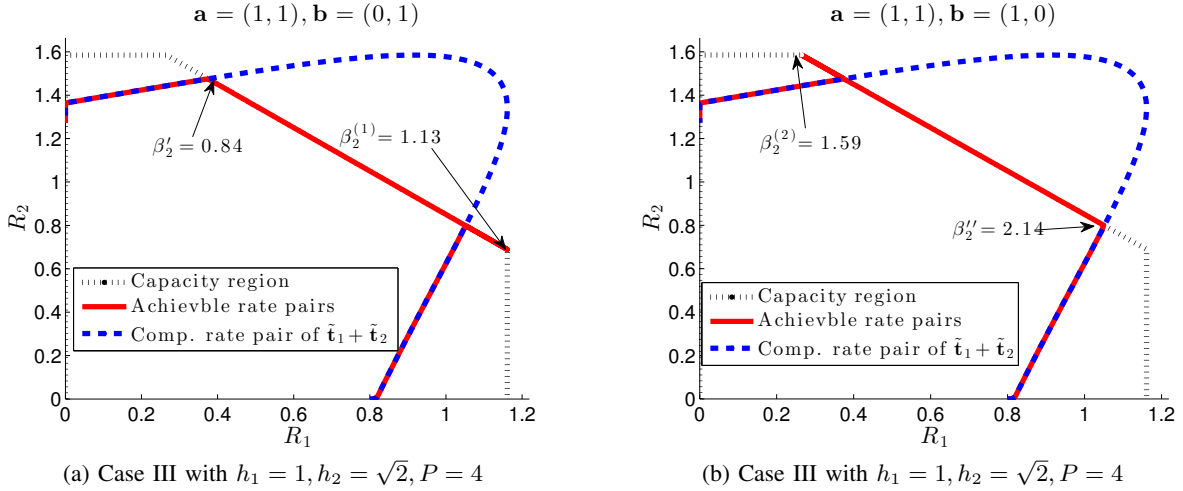


Fig. 4. Achievable rate pairs in Case III. The capacity region and the computation rate pairs in the two plots are the same. In this case the condition (37) is satisfied hence the computation rate pair of the first sum is large enough to achieve the whole capacity region by decoding two nontrivial integer sums. Plot (a) shows the achievable rate pairs by choosing $\mathbf{a} = (1, 1)$, $\mathbf{b} = (0, 1)$ and varying $\beta_2 \in [\beta'_2, \beta''_2]$. Plot (b) shows the achievable rate pairs by choosing $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 0)$ and varying $\beta_2 \in [\beta'_2, \beta''_2]$. The union of the achievable rate pairs with coefficients cover the whole dominant face of the capacity region. Recall that we have studied the achievable computation rate region for this channel in Figure 2.

A. On the choice of coefficients

In Theorem 3 we only considered the coefficients $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 0)$ or $\mathbf{b} = (0, 1)$. It is natural to ask whether choosing other coefficients could be advantageous.

We first consider when the coefficients \mathbf{a} of the first sum is chosen differently.

Lemma 2 (Achieving capacity with a different \mathbf{a}): Consider a 2-user Gaussian MAC where the receiver decodes two integer sums of the codewords with coefficients $\mathbf{a} = (a_1, a_2)$ and $\mathbf{b} = (0, 1)$ or $\mathbf{b} = (1, 0)$. Certain rate pairs

on the dominant face are achievable if it holds that

$$\frac{h_1 h_2 P}{\sqrt{1 + (h_1^2 + h_2^2)P}} \geq \frac{4a_1^2 a_2^2 - 1}{4a_1 a_2} \quad (54)$$

Furthermore the corner points of the capacity region are achievable if it holds that

$$\frac{h_1 h_2 P}{\sqrt{1 + (h_1^2 + h_2^2)P}} \geq a_1 a_2 \quad (55)$$

Proof: The proof of the first statement is given in the proof of Theorem 3, see Eqn. (47). The proof of the second statement is omitted as it is the same as the proof of Case III in Theorem 3 with a general \mathbf{a} . ■

This result suggests that although it is always possible to achieve the sum capacity with any \mathbf{a} , provided that the SNR of users are large enough, the choice $\mathbf{a} = (1, 1)$ is the best, in the sense that it requires the lowest SNR threshold, above which the sum capacity or the whole capacity region is achievable.

To illustrate this, let us reconsider the setting of Fig. 4, but now select the coefficients \mathbf{a} different from $(1, 1)$. As can be seen in Figure 6a, it is not possible to achieve sum capacity with $\mathbf{a} = (1, 2)$ or $\mathbf{a} = (2, 1)$. As we increase the power from $P = 4$ to $P = 10$, part of the capacity boundary is achieved, as shown in Figure 6b. However in this case we cannot achieve the whole capacity region. The reason lies in the fact that the computation rate pairs are different for $\mathbf{a} = (1, 2)$ and $\mathbf{a} = (2, 1)$.

Now we consider a different choice on the coefficients \mathbf{b} of the second sum. Although from the perspective of solving equations, having two sums with coefficients $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 0)$ or $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 2)$ is equivalent, here it is very important to choose \mathbf{b} such that it has one zero entry. Recall the result in Theorem 2 that if $b_k \neq 0$ for $k = 1, 2$, then both message rates R_1, R_2 will have two constraints from the two sums we decode. This extra constraint will diminish the achievable rate region, and in particular it only achieves some isolated points on the dominant face. This is illustrated by the example in Figure 7.

As a rule of thumb, the receiver should always decode the sums whose coefficients are as small as possible in a Gaussian MAC.

IV. THE K-USER GAUSSIAN MAC

In this section we consider the general K -user Gaussian MAC given in (1). Continuing with the coding scheme for the 2-user Gaussian MAC, in this case the receiver decodes K integer sums with linearly independent coefficients

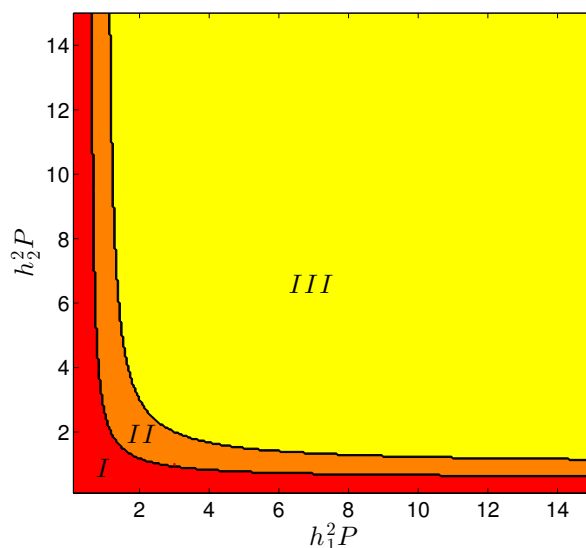


Fig. 5. The plane of the received SNR $h_1^2 P, h_2^2 P$ is divided into three regions. Region I corresponds to Case I when the condition (32) holds and the scheme cannot achieve points on the boundary of the capacity region. In Region II the condition (33) is met but the condition (37) is not, hence only part of the points on the capacity boundary can be achieved. Region III corresponds to Case III where (37) are satisfied and the proposed scheme can achieve any point in the capacity region.

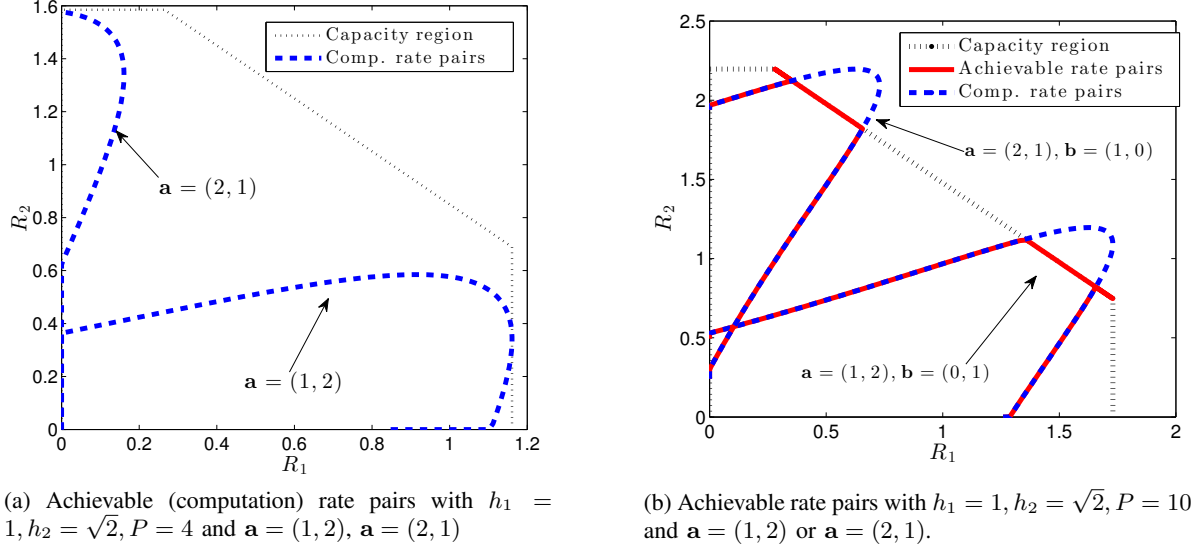


Fig. 6. In the left plot we show the computation rate pairs with parameters $h_1 = 1, h_2 = \sqrt{2}, P = 4$ where the coefficients of the first sum are chosen to be $\mathbf{a} = (1, 2)$ or $\mathbf{a} = (2, 1)$. In this case the condition (54) is not satisfied hence no point on the dominant face can be achieved for the first sum. Compare it to the example in Figure 4a or 4b where $\mathbf{a} = (1, 1)$ and the whole capacity region is achievable. We also note that the achievable computation rate pairs depicted in the Figure are also achievable message rate pairs, which can be shown using Theorem 2. In the right plot we show the achievable rate pairs with parameters $h_1 = 1, h_2 = \sqrt{2}, P = 10$ where the coefficient of the first sum is chosen to be $\mathbf{a} = (1, 2)$ or $\mathbf{a} = (2, 1)$. It can be checked with Lemma 2 that we can achieve the sum capacity with the given system parameters. Notice that only parts of the capacity boundary are achievable and we cannot obtain the whole dominant face in this case. In contrast, choosing $\mathbf{a} = (1, 1)$ achieves the whole dominant face.

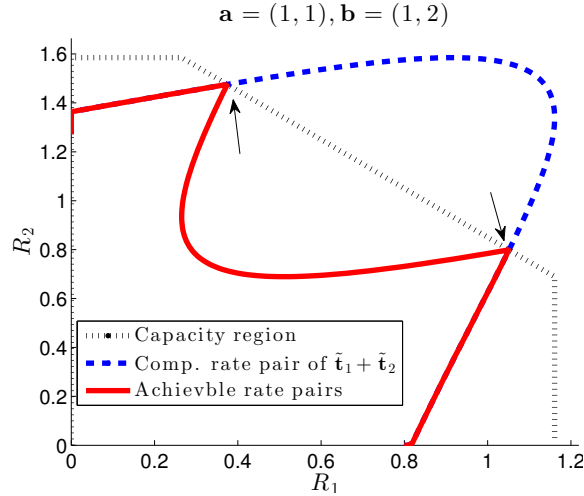


Fig. 7. The achievable rate pairs with parameters $h_1 = 1, h_2 = \sqrt{2}, P = 4$. In this case the condition (37) is satisfied hence the first sum is chosen properly. But as we choose $\mathbf{b} = (1, 2)$, only two isolated points (indicated by arrows) on the dominant face can be achieved. This is due to the fact non-zero entries in \mathbf{b} will give an extra constraint on the rate, cf. Theorem 2. Compare it to the example in Figure 4b.

and uses them to solve for the individual messages. The coefficients of the K sums will be denoted by a *coefficient matrix* $\mathbf{A} \in \mathbb{Z}^{K \times K}$

$$\mathbf{A} := (\mathbf{a}_1^T \dots \mathbf{a}_K^T)^T = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1K} \\ a_{21} & a_{22} & \dots & a_{2K} \\ \dots & \dots & \dots & \dots \\ a_{K1} & a_{K2} & \dots & a_{KK} \end{pmatrix} \quad (56)$$

where the row vector $\mathbf{a}_\ell := (a_{\ell 1}, \dots, a_{\ell K}) \in \mathbb{Z}^{1 \times K}$ denotes the coefficients of the ℓ -th sum, $\sum_{k=1}^K a_{\ell k} \tilde{\mathbf{t}}_k$, the receiver decodes.

The following theorem gives an achievable message rate tuple for the general K -user Gaussian MAC. It is an extension of [8, Thm. 2] as the scaling parameters β_k in our proposed scheme allow a larger achievable rate region.

Theorem 4 (Achievable message rate tuples for the K -user Gaussian MAC): Consider the K -user Gaussian MAC in (1). Let \mathbf{A} be a full-rank integer matrix and β_1, \dots, β_K be K non-zero real numbers. We define $\mathbf{B} := \text{diag}(\beta_1, \dots, \beta_K)$ and

$$\mathbf{K}_{\mathbf{Z}'} := P\mathbf{A}\mathbf{B}(\mathbf{I} + P\mathbf{h}\mathbf{h}^T)^{-1}\mathbf{B}^T\mathbf{A}^T \quad (57)$$

Let the matrix \mathbf{L} be the unique Cholesky factor of the matrix $\mathbf{A}\mathbf{B}(\mathbf{I} + P\mathbf{h}\mathbf{h}^T)^{-1}\mathbf{B}^T\mathbf{A}^T$, i.e.

$$\mathbf{K}_{\mathbf{Z}'} = P\mathbf{L}\mathbf{L}^T \quad (58)$$

The message rate tuple (R_1, \dots, R_K) is achievable with

$$R_k = \min_{\ell \in [1:K]} \left\{ \frac{1}{2} \log^+ \left(\frac{\beta_k^2}{L_{\ell\ell}^2} \right) \cdot \chi(a_{\ell k}) \right\}, k = 1, \dots, K \quad (59)$$

where we define

$$\chi(x) = \begin{cases} +\infty & \text{if } x = 0, \\ 1 & \text{otherwise.} \end{cases} \quad (60)$$

Furthermore if \mathbf{A} is a unimodular ($|\mathbf{A}| = 1$) and R_k is of the form

$$R_k = \frac{1}{2} \log \left(\frac{\beta_k^2}{L_{\Pi(k)\Pi(k)}^2} \right), k = 1, \dots, K \quad (61)$$

for some permutation Π of the set $\{1, \dots, K\}$, then the sum rate satisfies

$$\sum_k R_k = C_{\text{sum}} := \frac{1}{2} \log(1 + \sum_k h_k^2 P) \quad (62)$$

Proof: To proof this result, we will adopt a more compact representation and follow the proof technique given in [8]. We rewrite the system in (1) as

$$\mathbf{Y} = \mathbf{h}\mathbf{X} + \mathbf{z} \quad (63)$$

with $\mathbf{h} = (h_1, \dots, h_K) \in \mathbb{R}^{1 \times K}$ and $\mathbf{X} = (\mathbf{x}_1^T \dots \mathbf{x}_K^T)^T \in \mathbb{R}^{K \times n}$ where each $\mathbf{x}_k \in \mathbb{R}^{1 \times n}$ is the transmitted signal sequence of user k given by

$$\mathbf{x}_k = [\mathbf{t}_k / \beta_k + \mathbf{d}_k] \bmod \Lambda_k / \beta_k \quad (64)$$

Similar to the derivation for the 2-user case, we multiply the channel output by a matrix $\mathbf{F} \in \mathbb{R}^{K \times 1}$ and it can be shown that the following equivalent output can be obtained

$$\tilde{\mathbf{Y}} = \mathbf{A}\mathbf{T} + \tilde{\mathbf{Z}} \quad (65)$$

where $\mathbf{T} := (\tilde{\mathbf{t}}_1^T \dots \tilde{\mathbf{t}}_K^T)^T \in \mathbb{R}^{K \times n}$ and the lattice codeword $\tilde{\mathbf{t}}_k \in \mathbb{R}^{n \times 1}$ of user k is the same as defined in (21). Furthermore the noise $\tilde{\mathbf{Z}} \in \mathbb{R}^{K \times n}$ is given by

$$\tilde{\mathbf{Z}} = (\mathbf{F}\mathbf{h} - \mathbf{A}\mathbf{B})\mathbf{X} + \mathbf{F}\mathbf{z} \quad (66)$$

where $\mathbf{B} := \text{diag}(\beta_1, \dots, \beta_K)$. The matrix \mathbf{F} is chosen to minimize the variance of the noise:

$$\mathbf{F} := P\mathbf{A}\mathbf{B}\mathbf{h}^T \left(\frac{1}{P}\mathbf{I} + \mathbf{h}\mathbf{h}^T \right)^{-1} \quad (67)$$

As shown in the proof of [1, Thm. 5], when analyzing the lattice decoding for the system given in (65), we can consider the system

$$\tilde{\mathbf{Y}} = \mathbf{A}\mathbf{T} + \mathbf{Z}' \quad (68)$$

where $\mathbf{Z}' \in \mathbb{R}^{K \times n}$ is the equivalent noise and each row \mathbf{z}_k is a n -sequence of i.i.d Gaussian random variables z_k for $k = 1, \dots, K$. The covariance matrix of the Gaussians z_1, \dots, z_K is the same as that of the original noise \mathbf{Z} in (65). It is easy to show that the covariance matrix of the equivalent noise z_1, \dots, z_K is given in Eq. (57).

Now instead of doing the successive interference cancellation as in the 2-user case, we use an equivalent formulation which is called “noise prediction” in [8]. Because the matrix $\mathbf{A}\mathbf{B}(\mathbf{I} + P\mathbf{h}\mathbf{h}^T)^{-1}\mathbf{B}^T\mathbf{A}^T$ is positive definite, it admits the Cholesky factorization hence the covariance matrix $\mathbf{K}_{\mathbf{Z}'}$ can be rewritten as

$$\mathbf{K}_{\mathbf{Z}'} = P\mathbf{L}\mathbf{L}^T \quad (69)$$

where \mathbf{L} is a lower triangular matrix.

Using the Cholesky decomposition of $\mathbf{K}_{\mathbf{Z}'}$, the system (68) can be represented as

$$\tilde{\mathbf{Y}} = \mathbf{A}\mathbf{T} + \sqrt{P}\mathbf{L}\mathbf{W} \quad (70)$$

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1K} \\ a_{22} & a_{22} & \dots & a_{2K} \\ \vdots & \vdots & \vdots & \vdots \\ a_{K1} & a_{K2} & \dots & a_{KK} \end{pmatrix} \begin{pmatrix} \tilde{\mathbf{t}}_1 \\ \tilde{\mathbf{t}}_2 \\ \vdots \\ \tilde{\mathbf{t}}_K \end{pmatrix} + \sqrt{P} \begin{pmatrix} L_{11} & 0 & 0 & \dots & 0 \\ L_{21} & L_{22} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ L_{K1} & L_{K2} & L_{K3} & \dots & L_{KK} \end{pmatrix} \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \\ \vdots \\ \mathbf{w}_K \end{pmatrix} \quad (71)$$

with $\mathbf{W} = [\mathbf{w}_1^T, \dots, \mathbf{w}_K^T] \in \mathbb{R}^{K \times n}$ where $\mathbf{w}_i \in \mathbb{R}^{n \times 1}$ is an n -length sequence whose components are i.i.d. zero-mean white Gaussian random variables with unit variance. This is possible by noticing that $\sqrt{P}\mathbf{L}\mathbf{W}$ and \mathbf{Z}' have the same covariance matrix. Now we apply lattice decoding to each row of the above linear system. The first row of the equivalent system in (71) is given by

$$\tilde{\mathbf{y}}_1 := \mathbf{a}_1\mathbf{T} + \sqrt{P}L_{11}\mathbf{w}_1 \quad (72)$$

Using lattice decoding, the first integer sum $\mathbf{a}_1\mathbf{T} = \sum_k a_{1k}\tilde{\mathbf{t}}_k$ can be decoded reliably if

$$r_k < \frac{1}{2} \log^+ \frac{\beta_k^2 P}{PL_{11}^2} = \frac{1}{2} \log^+ \frac{\beta_k^2}{L_{11}^2} \quad (73)$$

Notice that if a_{1k} equals zero, the lattice point $\tilde{\mathbf{t}}_k$ does not participate in the sum $\mathbf{a}_1\mathbf{T}$ hence R_k is not constrained as above.

The important observation is that knowing $\mathbf{a}_1\mathbf{T}$ allows us to recover the noise term \mathbf{w}_1 from $\tilde{\mathbf{y}}_1$. This “noise prediction” is equivalent to the successive interference cancellation, see also [8]. Hence we could eliminate the term \mathbf{w}_1 in the second row of the system (71) to obtain

$$\tilde{\mathbf{y}}_2 := \mathbf{a}_2\mathbf{T} + \sqrt{P}L_{22}\mathbf{w}_2 \quad (74)$$

The lattice decoding of $\mathbf{a}_2\mathbf{T}$ is successful if

$$r_k < \frac{1}{2} \log^+ \frac{\beta_k^2 P}{PL_{22}^2} = \frac{1}{2} \log^+ \frac{\beta_k^2}{L_{22}^2} \quad (75)$$

Using the same idea we can eliminate all noise terms $\mathbf{w}_1, \dots, \mathbf{w}_{\ell-1}$ when decode the ℓ -th sum. Hence the rate constraints on k -th user when decoding this sum is given by

$$r_k < \frac{1}{2} \log^+ \frac{\beta_k^2 P}{PL_{\ell\ell}^2} = \frac{1}{2} \log^+ \frac{\beta_k^2}{L_{\ell\ell}^2} \quad (76)$$

When decoding the ℓ -th sum, the constraint on R_k will be active only if the coefficient of $\tilde{\mathbf{t}}_k$ is not zero. Otherwise this decoding will not constraint R_k . This fact is captured by introducing the χ function in the statement of the Theorem. Combing the above results and Lemma 1 we have the claimed expression.

In the case when R_k is of the form

$$R_k = \frac{1}{2} \log \left(\frac{\beta_k^2}{L_{\Pi(k)\Pi(k)}^2} \right) \quad (77)$$

The sum rate is

$$\sum_k R_k = \sum_k \frac{1}{2} \log \frac{\beta_k^2}{L_{\Pi(k)\Pi(k)}^2} = \frac{1}{2} \log \prod_k \frac{\beta_k^2}{L_{kk}^2} \quad (78)$$

$$= \frac{1}{2} \log \frac{\prod_k \beta_k^2}{|\mathbf{L}\mathbf{L}^T|} = \frac{1}{2} \log \frac{\prod_k \beta_k^2}{|\mathbf{A}\mathbf{B}(\mathbf{I} + \mathbf{P}\mathbf{h}\mathbf{h}^T)^{-1}\mathbf{B}^T\mathbf{A}^T|} \quad (79)$$

$$= \frac{1}{2} \log |\mathbf{I} + \mathbf{P}\mathbf{h}\mathbf{h}^T| + \frac{1}{2} \log \prod_k \beta_k^2 - \log |\mathbf{A}| - \frac{1}{2} \log |\mathbf{B}^T\mathbf{B}| \quad (80)$$

$$= \frac{1}{2} \log |\mathbf{I} + \mathbf{P}\mathbf{h}\mathbf{h}^T| - \log |\mathbf{A}| \quad (81)$$

$$= C_{sum} - \log |\mathbf{A}| \quad (82)$$

If \mathbf{A} is unimodular, i.e., $|\mathbf{A}| = 1$, the sum rate is equal to the sum capacity. \blacksquare

Remark 4: The theorem says that to achieve the sum capacity, we need \mathbf{A} to be unimodular and R_k should have the form $R_k = \frac{1}{2} \log \frac{\beta_k^2}{L_{\Pi(k)\Pi(k)}^2}$, whose validity of course depends on the choice of \mathbf{A} . It is difficult to characterize the class of \mathbf{A} for which this holds. In the case when \mathbf{A} is upper triangular with non-zero diagonal entries and $L_{11}^2 \leq \dots \leq L_{KK}^2$, this condition holds and in fact in this case we have $R_k = \frac{1}{2} \log \frac{\beta_k^2}{L_{kk}^2}$. It can be seen that we are exactly in this situation when we study the 2-user MAC in Theorem 3.

A. An example of a 3-user MAC

It is in general difficult to analytically characterize the achievable rate using our scheme of the K -user MAC. We give an example of a 3-user MAC in Figure 8 to help visualize the achievable region. The channel has the form $\mathbf{y} = \sum_{k=1}^3 \mathbf{x}_k + \mathbf{z}$ and the receiver decodes three sums with coefficients of the form

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ & \mathbf{e}_i & \\ & & \mathbf{e}_j \end{pmatrix} \quad (83)$$

for $i, j = 1, 2, 3$ and $i \neq j$ where \mathbf{e}_i is a row vector with 1 in its i -th and zero otherwise. It is easy to see that there are in total 6 matrices of this form and they all satisfy $|\mathbf{A}| = 1$ hence it is possible to achieve the capacity of this MAC according to Theorem 4. For power $P = 8$, most parts of the dominant face are achievable except for three triangular regions. For smaller power $P = 2$, the achievable part of the dominant face shrinks and particularly the symmetric capacity point is not achievable. It can be checked that in this example, no other coefficients will give a larger achievable region.

Unlike the 2-user case, even with a large power, not the whole dominant face can be obtained in this symmetric 3-user MAC. To obtain some intuition why it is the case, we consider one edge of the dominant face indicated by the arrow in Figure 8a. If we want to achieve the rate tuple on this edge, we need to decode user 1 last because R_1 attains its maximum. Hence a reasonable choice of the coefficients matrix would be

$$\mathbf{A}' = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \text{ or } \mathbf{A}' = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad (84)$$

Namely we first decode two sums to solve both \mathbf{t}_2 and \mathbf{t}_3 , and then decode \mathbf{t}_1 without any interference. When decoding the first two sums, we are effectively dealing with a 2-user MAC while treating \mathbf{t}_1 as noise. But the problem is that with \mathbf{t}_1 as noise, the signal-to-noise ratio of user 2 and 3 are too high, such that computation rate pair cannot reach the dominant face of the effective 2-user MAC with \mathbf{t}_1 being noise. This is the same situation as the Case I considered in Theorem 3. We also plot the achievable rates with the coefficients \mathbf{A}' above in Figure 8a on the side face. On the side face where R_1 attains its maximal value, we see the achievable rates cannot reach the dominant face, as a reminiscence of the 2-user example in Figure 3a.

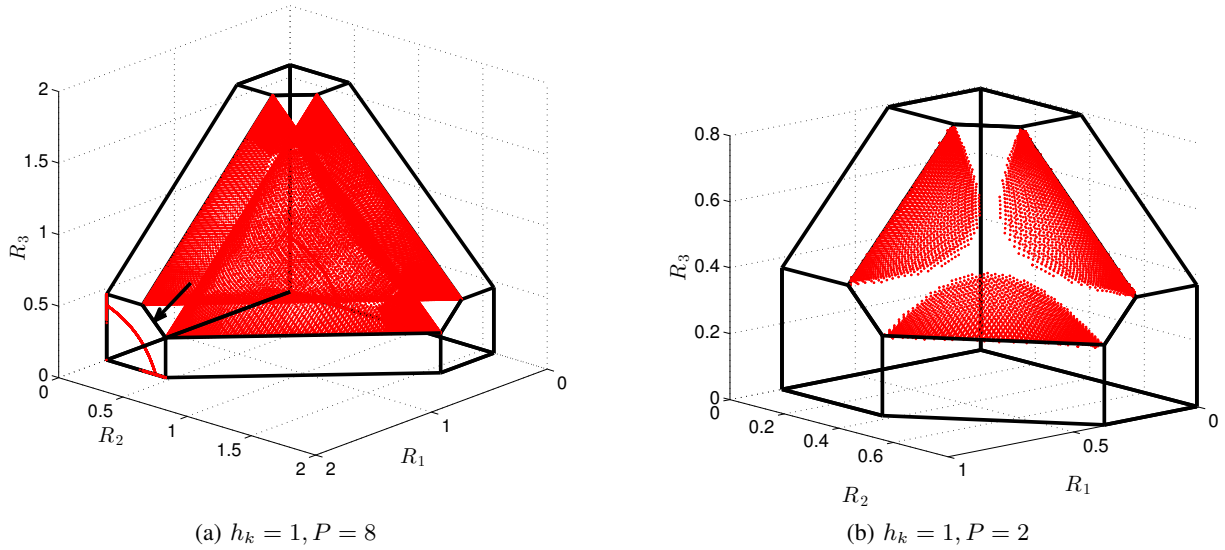


Fig. 8. The achievable rate region (red part) in Theorem 4 for a symmetric 3-user Gaussian MAC with $h_k = 1$ for $k = 1, 2, 3$ and different powers P .

B. The symmetric capacity for the symmetric Gaussian MAC

As it is difficult to obtain a complete description of the achievable rate region for a K -user MAC, in this section we investigate the simple symmetric channel where all the channel gains are the same. In this case we can absorb the channel gain into the power constraint and assume without loss of generality the channel model to be

$$\mathbf{y} = \sum_k \mathbf{x}_k + \mathbf{z} \quad (85)$$

where the transmitted signal \mathbf{x}_k has an average power constraint P . We want to see if the proposed scheme can achieve the symmetric capacity

$$C_{sym} = \frac{1}{2K} \log(1 + KP) \quad (86)$$

For this specific goal, we will fix our coefficient matrix to be

$$\mathbf{A} := \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (87)$$

Namely we first decode a sum involving all codewords $\sum_k \mathbf{t}_k$, then decode the individual codewords one by one. Due to symmetry the order of the decoding procedure is irrelevant and we fix it to be $\mathbf{t}_2, \dots, \mathbf{t}_K$. As shown in Theorem 4, the analysis of this problem is closely connected to the Cholesky factor \mathbf{L} defined in (58). This connection can be made more explicit if we are interested in the symmetric capacity for the symmetric channel.

We define

$$\mathbf{C} := \begin{pmatrix} 1 & \beta_2 & \beta_3 & \dots & \beta_K \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (88)$$

and \mathbf{E} to be the all-one matrix. Let the lower triangular matrix $\tilde{\mathbf{L}}$ denote the unique Cholesky factorization of the matrix $\mathbf{C}(\mathbf{I} - \frac{P}{1+KP}\mathbf{E})\mathbf{C}^T$, i.e.,

$$\mathbf{C} \left(\mathbf{I} - \frac{P}{1+KP}\mathbf{E} \right) \mathbf{C}^T = \tilde{\mathbf{L}}\tilde{\mathbf{L}}^T \quad (89)$$

Proposition 1 (Symmetric capacity): If there exist real numbers $\beta_2, \dots, \beta_K \geq 1$ with $|\beta_k| \geq 1$ such that the diagonal entries of $\tilde{\mathbf{L}}$ given in (89) are equal in amplitude i.e., $|\tilde{L}_{kk}| = |\tilde{L}_{jj}|$ for all k, j , then the symmetric capacity, i.e., $R_k = C_{\text{sym}}$ for all k , is achievable for the symmetric K -user Gaussian MAC.

Proof: Recall we have $\mathbf{B} = \text{diag}(\beta_1, \beta_2, \dots, \beta_K)$. Let \mathbf{A} be as given in (87) and the channel coefficients \mathbf{h} be the all-one vector. Substituting them into (57), (58) gives

$$P\tilde{\mathbf{C}} \left(\mathbf{I} - \frac{P}{1 + KP} \right) \tilde{\mathbf{C}}^T = P\mathbf{L}\mathbf{L}^T \quad (90)$$

where

$$\tilde{\mathbf{C}} = \begin{pmatrix} \beta_1 & \beta_2 & \beta_3 & \dots & \beta_K \\ 0 & \beta_2 & 0 & \dots & 0 \\ 0 & 0 & \beta_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & 0 & \beta_K \end{pmatrix} \quad (91)$$

In this case the we are interested in the Cholesky factorization \mathbf{L} above. Due to the special structure of \mathbf{A} chosen in (87), Theorem 4 implies that the following rates are achievable

$$R_1 = \frac{1}{2} \log \frac{\beta_1^2}{L_{11}^2} \quad (92)$$

$$R_k = \min \left\{ \frac{1}{2} \log \frac{\beta_k^2}{L_{11}^2}, \frac{1}{2} \log \frac{\beta_k^2}{L_{kk}^2} \right\}, k \geq 2 \quad (93)$$

Using the same argument in the proof of Theorem 4, it is easy to show that the sum capacity is achievable if $L_{kk}^2 \geq L_{11}^2$ for all $k \geq 2$. In the case of symmetric capacity we further require that

$$\frac{\beta_k^2}{L_{kk}^2} = \frac{\beta_j^2}{L_{jj}^2} \quad (94)$$

for all k, j . This is the same as requiring $\mathbf{B}^{-1}\mathbf{L}$ to have diagonals equal in amplitude with \mathbf{L} given in (90), or equivalently requiring the matrix $\mathbf{B}^{-1}\mathbf{A}\mathbf{B}(\mathbf{I} + P\mathbf{h}\mathbf{h}^T)^{-1}\mathbf{B}^T\mathbf{A}^T\mathbf{B}^{-T}$ having Cholesky factorization whose diagonals are equal in amplitude. We can let $\beta_1 = 1$ without loss of generality and it is straightforward to check that in this case $\mathbf{B}^{-1}\mathbf{A}\mathbf{B} = \mathbf{C}$. Now the condition in (94) is equivalently represented as

$$\tilde{L}_{kk}^2 = \tilde{L}_{jj}^2 \quad (95)$$

and the requirement $L_{kk}^2 \geq L_{11}^2$ for $k \geq 2$ can be equivalently written as $\beta_k^2 \geq \beta_1^2 = 1$. ■

We point out that the value of power P plays a key role in Proposition 1. It is not true that for any power constraint P , there exists β_2, \dots, β_K such that the equality condition in Proposition 1 can be fulfilled. For the two user case analyzed in Section III, we can show that for the symmetric channel, the equality condition in Proposition 1 can be fulfilled if the condition (33) holds, which in turn requires $P \geq 1.5$ for the symmetric channel. In general for a given K , we expect that there exists a threshold $P^*(K)$ such that for $P \geq P^*(K)$, we can always find β_2, \dots, β_K which satisfy the equality condition in Proposition 1 hence achieve the symmetric capacity. This can be formulated as follows.

Conjecture 1 (Achievability of the symmetric capacity): For any $K \geq 2$, there exists a positive number $P^*(K)$, such that for $P \geq P^*(K)$, we can find real numbers β_2, \dots, β_K , where $|\beta_k| \geq 1$ with which the diagonal entries of $\tilde{\mathbf{L}}$ given in (89) are equal in amplitude i.e., $|\tilde{L}_{kk}| = |\tilde{L}_{jj}|$ for all k, j .

We have not been able to prove this claim. Table I gives some numerical results for the choices of $\underline{\beta}$ which achieve the symmetric capacity in a K -user Gaussian MAC with power constraint $P = 15$ and different values of K . With this power constraint the claim in Conjecture 1 is numerically verified with K up to 6. Notice that the value β_k decreases with the index k for $k \geq 2$. This is because with the coefficient matrix \mathbf{A} in (87), the decoding order of the individual users is from 2 to K (and user 1 is decoded last). The earlier the message is decoded, the larger the corresponding β will be.

Some numerical results for $P^*(K)$ for K up to 5 is given in Table II. As we have seen $P^*(2) = 1.5$. For other K we give the interval which contains $P^*(K)$ by numerical evaluations.

TABLE I
THE CHOICE OF $\underline{\beta}$ FOR A K -USER GAUSSIAN MAC WITH POWER $P = 15$.

K	β_1	β_2	β_3	β_4	β_5	β_6
2	1	1.1438				
3	1	1.5853	1.2582			
4	1	1.6609	1.3933	1.1690		
5	1	1.6909	1.4626	1.2796	1.1034	
6	1	1.6947	1.4958	1.3361	1.1980	1.0445

TABLE II
THE INTERVALS CONTAINING $P^*(K)$

K	$P^*(K)$
2	1.5
3	[2.23, 2.24]
4	[3.74, 3.75]
5	[7.07, 7.08]

V. THE 2-USER GAUSSIAN DIRTY MAC

In the previous sections we focused on the standard Gaussian multiple access channels. In this section we will consider the Gaussian MAC with interfering signals which are non-causally known at the transmitters. This channel model is called Gaussian “dirty MAC” and is studied in [9]. Some related results are given in [18], [19], [20]. A two-user Gaussian dirty MAC is given by

$$\mathbf{y} = h_1 \mathbf{x}_1 + h_2 \mathbf{x}_2 + \mathbf{s}_1 + \mathbf{s}_2 + \mathbf{z} \quad (96)$$

where the assumption on $\mathbf{x}_1, \mathbf{x}_2$ and \mathbf{z} are the same as for the standard Gaussian MAC in (1). The interference \mathbf{s}_k is a zero-mean i.i.d. Gaussian random sequence with variance Q_k for each entry, $k = 1, 2$. An important assumption is that the interference signal \mathbf{s}_k is only non-causally known to transmitter k . Two users need to mitigate two interference signals in a distributed manner, which makes this problem challenging. By letting $Q_1 = Q_2 = 0$ we recover the standard Gaussian MAC.

This problem can be seen as an extension of the well-known dirty-paper coding problem [21] to the multiple-access channels. However as shown in [9], a straightforward extension of the usual Gelfand-Pinsker scheme [22] is not optimal and in the limiting case when interference is very strong, the achievable rates are zero. Although the capacity region of this channel is unknown in general, it is shown in [9] that lattice codes are well-suited for this problem and give better performance than the usual random coding scheme.

Now we will extend our coding scheme in previous sections to the dirty MAC. The basic idea is still to decode two linearly independent sums of the codewords. The new ingredient is to mitigate the interference $\mathbf{s}_1, \mathbf{s}_2$ in the context of lattice codes. For a point-to-point AWGN channel with interference known non-causally at the transmitter, it has been shown that capacity can be attained with lattice codes [23]. Our coding scheme is an extension of the schemes in [23] and [9].

Theorem 5 (Achievability for the Gaussian dirty MAC): For the dirty multiple access channel given in (96), the following message rate pair is achievable

$$R_k = \begin{cases} r_k(\mathbf{a}, \underline{\gamma}, \underline{\beta}) & \text{if } b_k = 0 \\ r_k(\mathbf{b}|\mathbf{a}, \underline{\gamma}, \underline{\beta}) & \text{if } a_k = 0 \\ \min\{r_k(\mathbf{a}, \underline{\gamma}, \underline{\beta}), r_k(\mathbf{b}|\mathbf{a}, \underline{\gamma}, \underline{\beta})\} & \text{otherwise} \end{cases} \quad (97)$$

for any linearly independent integer vectors $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^2$ and $\underline{\gamma}, \underline{\beta} \in \mathbb{R}^2$ if $r_k(\mathbf{a}, \underline{\gamma}, \underline{\beta}), r_k(\mathbf{b}|\mathbf{a}, \underline{\gamma}, \underline{\beta}) > 0$ for $k = 1, 2$,

whose expressions are given as

$$r_k(\mathbf{a}, \underline{\gamma}, \underline{\beta}) := \max_{\alpha_1} \frac{1}{2} \log^+ \frac{\beta_k^2 P_k}{N_1(\alpha_1, \underline{\gamma}, \underline{\beta})} \quad (98)$$

$$r_k(\mathbf{b}|\mathbf{a}, \underline{\gamma}, \underline{\beta}) := \max_{\alpha_2, \lambda} \frac{1}{2} \log^+ \frac{\beta_k^2 P_k}{N_2(\alpha_2, \underline{\gamma}, \underline{\beta}, \lambda)} \quad (99)$$

with

$$N_1(\alpha_1, \underline{\gamma}, \underline{\beta}) = \alpha_1^2 + \sum_k \left((\alpha_1 - a_k \beta_k)^2 P_k + (\alpha_1 - a_k \gamma_k)^2 Q_k \right) \quad (100)$$

$$N_2(\alpha_2, \underline{\gamma}, \underline{\beta}, \lambda) = \alpha_2^2 + \sum_k \left((\alpha_2 - \lambda a_k \gamma_k - b_k \gamma_k)^2 Q_k + (\alpha_2 - \lambda a_k \beta_k - b_k \beta_k)^2 P_k \right) \quad (101)$$

Proof: Let \mathbf{t}_k be the lattice codeword of user k and \mathbf{d}_k the dither uniformly distributed in \mathcal{V}_k^s/β_k . The channel input is given as

$$\mathbf{x}_k = [\mathbf{t}_k/\beta_k + \mathbf{d}_k - \gamma_k \mathbf{s}_k/\beta_k] \mod \Lambda_k^s/\beta_k$$

for some γ_k to be determined later. In Appendix C we show that with the channel output \mathbf{y} we can form

$$\tilde{\mathbf{y}}_1 := \tilde{\mathbf{z}}_1 + \sum_k a_k \tilde{\mathbf{t}}_k + \sum_k (\alpha_1 - a_k \gamma_k) \mathbf{s}_k \quad (102)$$

where α_1 is some real numbers to be optimized later and we define $\tilde{\mathbf{t}}_k := \mathbf{t}_k - Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k - \gamma_k \mathbf{s}_k)$ and $\tilde{\mathbf{z}}_1 := \sum_k (\alpha_1 - a_k \beta_k) \mathbf{x}_k + \alpha_1 \mathbf{z}$. Due to the nested lattice construction we have $\tilde{\mathbf{t}}_k \in \Lambda$. Furthermore the term $\tilde{\mathbf{z}}_1 + \sum_k (\alpha_1 - a_k \gamma_k) \mathbf{s}_k$ is independent of the sum $\sum_k a_k \tilde{\mathbf{t}}_k$ thanks to the dither and can be seen as the equivalent noise having average power per dimension $N_1(\alpha, \underline{\gamma}, \underline{\beta})$ in (100) for $k = 1, 2$. In order to decode the integer sum $\sum_k a_k \tilde{\mathbf{t}}_k$ we require

$$r_k < r_k(\mathbf{a}, \underline{\gamma}, \underline{\beta}) := \max_{\alpha_1} \frac{1}{2} \log^+ \frac{\beta_k^2 P_k}{N_1(\alpha_1, \underline{\gamma}, \underline{\beta})} \quad (103)$$

Notice this constraint on R_k is applicable only if $a_k \neq 0$.

If we can decode $\sum_k a_k \tilde{\mathbf{t}}_k$ with positive rate, the idea of successive interference cancellation can be applied. We show in Appendix C that for decoding the second sum we can form

$$\tilde{\mathbf{y}}_2 := \tilde{\mathbf{z}}_2 + \sum_k (\alpha_2 - \lambda a_k \gamma_k - b_k \gamma_k) \mathbf{s}_k + \sum_k b_k \tilde{\mathbf{t}}_k \quad (104)$$

where α_2 and λ are two real numbers to be optimized later and we define $\tilde{\mathbf{z}}_2 := \sum_k (\alpha_2 - \lambda a_k \beta_k - b_k \beta_k) \mathbf{x}_k + \alpha_2 \mathbf{z}$. Now the equivalent noise $\tilde{\mathbf{z}}_2 + \sum_k (\alpha_2 - \lambda a_k \gamma_k - b_k \gamma_k) \mathbf{s}_k$ has average power per dimension $N_2(\alpha_2, \underline{\gamma}, \underline{\beta}, \lambda)$ given in (101). Using lattice decoding we can show the following rate pair for decoding $\sum_k b_k \tilde{\mathbf{t}}_k$ is achievable

$$r_k < r_k(\mathbf{b}|\mathbf{a}, \underline{\gamma}, \underline{\beta}) := \max_{\alpha_2, \lambda} \frac{1}{2} \log^+ \frac{\beta_k^2 P_k}{N_2(\alpha_2, \underline{\gamma}, \underline{\beta}, \lambda)} \quad (105)$$

Again the lattice points $\tilde{\mathbf{t}}_k$ can be solved from the two sums if \mathbf{a} and \mathbf{b} are linearly independent, and \mathbf{t}_k is recovered by the modulo operation $\mathbf{t}_k = [\tilde{\mathbf{t}}_k] \mod \Lambda_k^s$ even if \mathbf{s}_k is not known at the receiver. Again if we have $b_k = 0$, the above constraint does not apply to R_k . ■

A. Decoding one integer sum

We revisit the results obtained in [9] and show they can be obtained in our framework in a unified way.

Theorem 6 ([9] Theorem 2, 3): For the dirty multiple access channel given in (96), we have the following achievable rate region:

$$R_1 + R_2 = \begin{cases} \frac{1}{2} \log(1 + \min\{P_1, P_2\}) & \text{if } \sqrt{P_1 P_2} - \min\{P_1, P_2\} \geq 1 \\ \frac{1}{2} \log^+ \left(\frac{P_1 + P_2 + 1}{2 + (\sqrt{P_1} - \sqrt{P_2})^2} \right) & \text{otherwise} \end{cases}$$

Remark 5: The above rate region was obtained by considering the transmitting scheme where only one user transmits at a time. In our framework, it is the same as assuming one transmitted signal, say \mathbf{t}_1 , is set to be $\mathbf{0}$ and known to the decoder. In this case we need only one integer sum to decode \mathbf{t}_2 . Here we give a proof to show the achievability for

$$R_2 = \begin{cases} \frac{1}{2} \log(1 + P_2) & \text{for } P_1 \geq \frac{(P_2+1)^2}{P_2} \\ \frac{1}{2} \log(1 + P_1) & \text{for } P_2 \geq \frac{(P_1+1)^2}{P_1} \\ \frac{1}{2} \log^+ \left(\frac{P_1+P_2+1}{2+(\sqrt{P_1}-\sqrt{P_2})^2} \right) & \text{otherwise} \end{cases} \quad (106)$$

while $R_1 = 0$. Theorem 6 is obtained by showing the same result holds when we switch the two users and a time-sharing argument.

Proof: Choosing $\mathbf{a} = (1, 1)$ and $\gamma_1 = \gamma_2 = \alpha_1$ in (103), we can decode the integer sum $\sum_k \tilde{\mathbf{t}}_k$ if

$$r_2 < r_2(\mathbf{a}, \underline{\beta}) = \frac{1}{2} \log \frac{P_2(1 + P_1 + P_2)}{r^2 P_1 + P_2 + P_1 P_2 (r - 1)^2} \quad (107)$$

by choosing the optimal $\alpha_1^* = \frac{\beta_1 P_1 + \beta_2 P_2}{P_1 + P_2 + 1}$ and defining $r := \beta_1 / \beta_2$. An important observation is that in order to extract \mathbf{t}_2 from the integer sum (assuming $\mathbf{t}_1 = \mathbf{0}$)

$$\sum_k \tilde{\mathbf{t}}_k = \mathbf{t}_2 - Q_{\Lambda_2^s}(\mathbf{t}_2 + \beta_2 \mathbf{d}_2 - \gamma_2 \mathbf{s}_2) - Q_{\Lambda_1^s}(\beta_1 \mathbf{d}_1 - \gamma_1 \mathbf{s}_1),$$

one sufficient condition is $\Lambda_1^s \subseteq \Lambda_2^s$. Indeed, due to the fact that $[\mathbf{x}] \bmod \Lambda_2^s = \mathbf{0}$ for any $\mathbf{x} \in \Lambda_1^s \subseteq \Lambda_2^s$, we are able to recover \mathbf{t}_2 by performing $[\sum_k \tilde{\mathbf{t}}_k] \bmod \Lambda_2^s$ if $\Lambda_1^s \subseteq \Lambda_2^s$. This requirement amounts to the condition $\beta_1^2 P_1 \geq \beta_2^2 P_2$ or equivalently $r \geq \sqrt{P_2/P_1}$. Notice if we can extract \mathbf{t}_2 from just one sum $\sum_k \tilde{\mathbf{t}}_k$ (with \mathbf{t}_1 known), then the computation rate $R_2^a = r_2(\mathbf{a}, \underline{\beta})$ will also be the message rate $R_2 = r_2(\mathbf{a}, \underline{\beta})$.

Taking derivative w. r. t. r in (107) gives the critical point

$$r^* = \frac{P_2}{P_2 + 1} \quad (108)$$

If $r^* \geq \sqrt{P_2/P_1}$ or equivalently $P_1 \geq \frac{(P_2+1)^2}{P_2}$, substituting r^* in (107) gives

$$R_2 = \frac{1}{2} \log(1 + P_2)$$

If $r^* \leq \sqrt{P_2/P_1}$ or equivalently $P_1 \leq \frac{(P_2+1)^2}{P_2}$, R_2 is non-increasing in r hence we should choose $r = \sqrt{P_2/P_1}$ to get

$$R_2 = \frac{1}{2} \log^+ \left(\frac{1 + P_1 + P_2}{2 + (\sqrt{P_2} - \sqrt{P_1})^2} \right) \quad (109)$$

To show the result for the case $P_2 \geq \frac{(P_1+1)^2}{P_1}$, we set the transmitting power of user 2 to be $P'_2 = \frac{(P_1+1)^2}{P_1}$ which is smaller or equal to its full power P_2 under this condition. In order to satisfy the nested lattice constraint $\Lambda_1^s \subseteq \Lambda_2^s$ we also need $\beta_1^2 P_1 \leq \beta_2^2 P'_2$ or equivalently $r \geq \sqrt{P'_2/P_1}$. By replacing P_2 by the above P'_2 and choosing $r = \sqrt{P'_2/P_1}$ in (107) we get

$$R_2 = \frac{1}{2} \log(1 + P_1) \quad (110)$$

Interestingly under this scheme, letting the transmitting power to be P'_2 gives a larger achievable rate than using the full power P_2 in this power regime. ■

An outer bound on the capacity region given in [9, Corollary 2] states that the sum rate capacity should satisfy

$$R_1 + R_2 \leq \frac{1}{2} \log(1 + \min\{P_1, P_2\}) \quad (111)$$

for strong interference (both Q_1, Q_2 go to infinity). Hence in the strong interference case, the above achievability result is either optimal (when P_1, P_2 are not too close) or only a constant away from the capacity region (when P_1, P_2 are close, see [9, Lemma 3]). However the rates in Theorem 6 are strictly suboptimal for general interference strength as we will show in the sequel.

B. Decoding two integer sums

Now we consider decoding two sums for the Gaussian dirty MAC by evaluating the achievable rates stated in Theorem 5. Unlike the case of the clean MAC studied in Section III, here we need to optimize over $\underline{\gamma}$ for given \mathbf{a}, \mathbf{b} and $\underline{\beta}$, which does not have a closed-form solution due to the $\min\{\cdot\}$ operation. Hence in this section we resort to numerical methods for evaluations. To give an example of the advantage for decoding two sums, we show achievable rate regions in Figure 9 for a dirty MAC where $P_1 = Q_1 = 10$ and $P_2 = Q_2 = 2$. We see in the case when the transmitting power and interference strength are comparable, decoding two sums gives a significantly larger achievable rate region. In this example we choose the coefficients to be $\mathbf{a} = (a_1, 1), \mathbf{b} = (1, 0)$ or $\mathbf{a} = (1, a_2), \mathbf{b} = (1, 0)$ for $a_1, a_2 = 1, \dots, 5$ and optimize over parameters $\underline{\gamma}$. We also point out that unlike the case of the clean MAC where it is best to choose a_1, a_2 to be 1, here choosing coefficients a_1, a_2 other than 1 gives larger achievable rate regions in general.

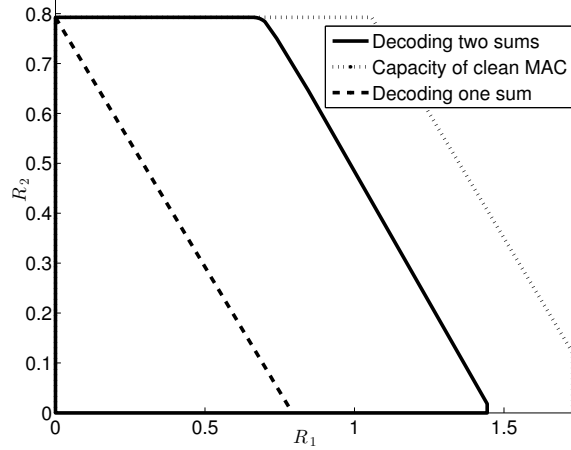


Fig. 9. We consider a dirty MAC with $P_1 = Q_1 = 10$ and $P_2 = Q_2 = 2$. The dashed line is the achievable rate region given in Theorem 6 from [9] which corresponds to decoding only one sum. The solid line gives the achievable rate region in Theorem 5 by decoding two sums with the coefficients $\mathbf{a} = (a_1, 1), \mathbf{b} = (1, 0)$ or $\mathbf{a} = (1, a_2), \mathbf{b} = (1, 0)$ for $a_1, a_2 = 1, \dots, 5$ and optimizing over parameters $\underline{\gamma}$.

Different from the point-to-point Gaussian channel with interference known at the transmitter, it is no longer possible to eliminate all interference completely without diminishing the capacity region for the dirty MAC. The proposed scheme provides us with a way of trading off between eliminating the interference and treating it as noise. Figure 10 shows the symmetric rate of the dirty MAC as a function of interference strength. When the interference is weak, the proposed scheme balances the residual interference s_1, s_2 in N_1 , see Eqn. (100) and N_2 , see Eqn. (101) by optimizing the parameters $\underline{\gamma}$. This is better than only decoding one sum in which we completely cancel out the interference.

As mentioned in the previous subsection, decoding one integer sum is near-optimal in the limiting case when both interference signals s_1, s_2 are very strong, i.e., $Q_1, Q_2 \rightarrow \infty$. It is natural to ask if we can do even better by decoding two sums in this case. It turns out in the limiting case we are not able to decode two linearly independent sums with this scheme.

Lemma 3 (Only one sum for high interference): For the 2-user dirty MAC in (96) with $Q_1, Q_2 \rightarrow \infty$, we have $r_k(\mathbf{a}, \underline{\gamma}, \underline{\beta}) = r_k(\mathbf{b}|\mathbf{a}, \underline{\gamma}, \underline{\beta}) = 0, k = 1, 2$ for any linearly independent \mathbf{a}, \mathbf{b} where $a_k \neq 0, k = 1, 2$.

Proof: The rate expressions in (103) and (105) show that we need to eliminate all terms involving Q_k in the equivalent noise N_1 in (100) and N_2 in (101), in order to have a positive rate when $Q_1, Q_2 \rightarrow \infty$. Consequently we need $\alpha_1 - a_k \gamma_k = 0$ and $\alpha_2 - \lambda a_k \gamma_k - b_k \gamma_k = 0$ for $k = 1, 2$. or equivalently

$$\begin{pmatrix} 1 & 0 & -a_1 & 0 \\ 0 & 1 & -\lambda a_1 - b_1 & 0 \\ 1 & 0 & 0 & -a_2 \\ 0 & 1 & 0 & -\lambda a_2 - b_2 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \gamma_1 \\ \gamma_2 \end{pmatrix} = \mathbf{0} \quad (112)$$

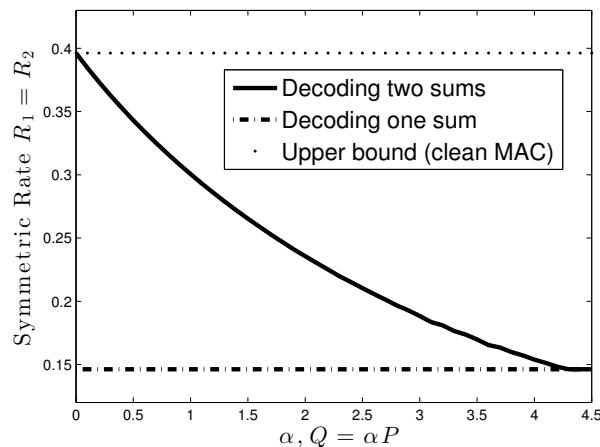


Fig. 10. We consider a dirty MAC with $P_1 = P_2 = 1$ and $Q_1 = Q_2 = \alpha P_1$ with different α varying from $[0, 4.5]$. The vertical axis denotes the maximum symmetric rate $R_1 = R_2$. The dotted line is the maximum symmetric rate $1/4 \log(1 + P_1 + P_2)$ for a clean MAC as an upper bound. The dashed line gives the achievable symmetric rate in Theorem 6 from [9] and the solid line depicts the symmetric rate in Theorem 5 by decoding two sums.

Performing elementary row operations gives the following equivalent system

$$\begin{pmatrix} 1 & 0 & -a_1 & 0 \\ 0 & 1 & -\lambda a_1 - b_1 & 0 \\ 0 & 0 & a_1 & -a_2 \\ 0 & 0 & 0 & \frac{a_2(\lambda a_1 + b_1)}{a_1} - \lambda a_2 - b_2 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \gamma_1 \\ \gamma_2 \end{pmatrix} = \mathbf{0} \quad (113)$$

To have non-trivial solutions of $\underline{\alpha}$ and $\underline{\gamma}$ with $a_1 \neq 0$, we must have $\frac{a_2(\lambda a_1 + b_1)}{a_1} - \lambda a_2 - b_2 = 0$, which simplifies to $a_2 b_1 = a_1 b_2$, meaning \mathbf{a} and \mathbf{b} are linearly dependent. ■

This observation suggests that when both interference signals are very strong, the strategy in [9] to let only one user transmit at a time (section V-A) is the best thing to do within this framework. However we point out that in the case when only one interference is very strong, we can still decode two independent sums with positive rates. For example consider the system in (96) with \mathbf{s}_2 being identically zero, \mathbf{s}_1 only known to User 1 and $Q_1 \rightarrow \infty$. In this case we can decode two linearly independent sums with $\mathbf{a} = (1, 1)$, $\mathbf{b} = (1, 0)$ or $\mathbf{a} = (1, 0)$, $\mathbf{b} = (0, 1)$. The resulting achievable rates with Theorem 5 is the same as that given in [9, Lemma 9]. Moreover, the capacity region of the dirty MAC with only one interference signal commonly known to both users [9, VIII] can also be achieved using Theorem 5, by choosing $\mathbf{a} = (1, 0)$, $\mathbf{b} = (0, 1)$ for example.

VI. CONCLUDING REMARKS

We have shown that the lattice code combined with a compute-and-forward technique is able to achieve the capacity of multiple access channels. This coding scheme is of possible practical interests because it only uses a single-user decoder without time-sharing or rate-splitting techniques. The proposed coding scheme is a generalization of the celebrated compute-and-forward technique and can be applied to many other Gaussian network scenarios. However as we have seen in the 2-user and 3-user examples, the capacity-achieving ability of this scheme fails if the signal-to-noise ratio is low. The reason lies in the fact that in this regime the computation rate pair is not large enough (recall the examples in Theorem 3). Hence it is interesting to ask what is the largest possible computation rate tuple in a Gaussian MAC. The answer to this question has implications on many other unsolved network communication problems, including the Gaussian interference channel and the Gaussian two-way relay channel.

APPENDIX A

THE PROOF OF THEOREM 1

A proof of the 2-user case of Theorem 1 is already contained in the proof of Theorem 2. We now give a proof for the K -user case.

When the message (codeword) \mathbf{t}_k is given to encoder k , it forms its channel input as follows

$$\mathbf{x}_k = [\mathbf{t}_k/\beta_k + \mathbf{d}_k] \bmod \Lambda_k^s/\beta_k \quad (114)$$

where the dither \mathbf{d}_k is a random vector uniformly distributed in the scaled Voronoi region \mathcal{V}_k^s/β_k . Notice that \mathbf{x}_k is independent from \mathbf{t}_k and also uniformly in Λ_k^s/β_k hence has average power P for all k .

At the decoder we form

$$\tilde{\mathbf{y}} := \alpha \mathbf{y} - \sum_k a_k \beta_k \mathbf{d}_k \quad (115)$$

$$= \sum_k a_k (\beta_k (\mathbf{t}_k/\beta_k + \mathbf{d}_k) - \beta_k Q_{\Lambda_k^s/\beta_k}(\mathbf{t}_k/\beta_k + \mathbf{d}_k)) - \sum_k a_k \beta_k \mathbf{d}_k + \tilde{\mathbf{z}} \quad (116)$$

$$\stackrel{(a)}{=} \tilde{\mathbf{z}} + \sum_k a_k (\mathbf{t}_k - Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k)) \quad (117)$$

$$:= \tilde{\mathbf{z}} + \sum_k a_k \tilde{\mathbf{t}}_k \quad (118)$$

with $\tilde{\mathbf{t}}_k := \mathbf{t}_k - Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k)$ and the equivalent noise

$$\tilde{\mathbf{z}} := \sum_k (\alpha h_k - a_k \beta_k) \mathbf{x}_k + \alpha \mathbf{z} \quad (119)$$

which is independent of $\sum_k a_k \tilde{\mathbf{t}}_k$ since all \mathbf{x}_k are independent of $\sum_k a_k \tilde{\mathbf{t}}_k$ thanks to the dithers \mathbf{d}_k . The step (a) follows because it holds $Q_{\Lambda}(\beta X) = \beta Q_{\frac{\Lambda}{\beta}}(X)$ for any $\beta \neq 0$. Notice we have $\tilde{\mathbf{t}}_k \in \Lambda$ since $\mathbf{t}_k \in \Lambda$ and $\Lambda_k^s \subseteq \Lambda$ due to the code construction. Hence the linear combination $\sum_k a_k \tilde{\mathbf{t}}_k$ along belongs to the decoding lattice Λ .

The decoder uses lattice decoding to obtain $\sum_k a_k \tilde{\mathbf{t}}_k$ with respect to the decoding lattice Λ by quantizing $\tilde{\mathbf{y}}$ to its nearest neighbor in Λ . The decoding error probability is equal to the probability that the equivalent noise $\tilde{\mathbf{z}}$ leaves the Voronoi region surrounding the lattice point representing $\sum_k a_k \tilde{\mathbf{t}}_k$. If the fine lattice Λ used for decoding is good for AWGN channel, as it is shown in [12], the probability $\Pr(\tilde{\mathbf{z}}_m \notin \mathcal{V})$ goes to zero exponentially if

$$\frac{\text{Vol}(\mathcal{V})^{2/n}}{N(\alpha)} > 2\pi e \quad (120)$$

where

$$N(\alpha) := \mathbb{E} \|\tilde{\mathbf{z}}\|^2 / n = \|\alpha \mathbf{h} - \tilde{\mathbf{a}}\|^2 P + \alpha^2 \quad (121)$$

denotes the average power per dimension of the equivalent noise. Recall that the shaping lattice Λ_k^s is good for quantization hence we have

$$\text{Vol}(\mathcal{V}_k^s) = \left(\frac{\beta_k^2 P}{G(\Lambda_k^s)} \right)^{n/2} \quad (122)$$

with $G(\Lambda_k^s) 2\pi e < (1 + \delta)$ for any $\delta > 0$ if n is large enough [12]. Together with the message rate expression in (5) we can see that lattice decoding is successful if $\beta_k^2 P 2^{-2R_k} / G(\Lambda_k^s) > 2\pi e N$ for every k , or equivalently

$$r_k < \frac{1}{2} \log \left(\frac{P}{N(\alpha)} \right) + \frac{1}{2} \log \beta_k^2 - \frac{1}{2} \log(1 + \delta)$$

By choosing δ arbitrarily small and optimizing over α we conclude that the lattice decoding of $\sum_k a_k \tilde{\mathbf{t}}_k$ will be successful if

$$r_k < \max_{\alpha} \frac{1}{2} \log \left(\frac{P}{N(\alpha)} \right) + \frac{1}{2} \log \beta_k^2 = R_k^a \quad (123)$$

with R_k^a given in (8). Finally, since there is a one-to-one mapping between $\tilde{\mathbf{t}}_k$ and \mathbf{t}_k when the dithers \mathbf{d}_k are known, we can also recover $\sum_k a_k \mathbf{t}_k$.

APPENDIX B
DERIVATIONS IN THE PROOF OF THEOREM 3

Here we prove the claim in Theorem 3 that $\beta_2^{(1)}, \beta_2^{(2)} \in [\beta_2', \beta_2'']$ if and only if the Condition (37) holds. Recall we have defined $\beta_2^{(1)} := \frac{h_1 h_2 P}{1+h_1^2 P}$, $\beta_2^{(2)} := \frac{1+h_2^2 P}{h_1 h_2 P}$ and β_2', β_2'' in Eqn. (44).

With the choice $\mathbf{a} = (1, 1)$ we can rewrite (44) as

$$\beta_2' := \frac{2h_1 h_2 P + S - \sqrt{SD}}{2(1 + h_1^2 P)} \quad (124)$$

$$\beta_2'' := \frac{2h_1 h_2 P + S + \sqrt{SD}}{2(1 + h_1^2 P)} \quad (125)$$

with $S := \sqrt{1 + h_1^2 P + h_2^2 P}$ and $D := 4Ph_1 h_2 - 3S$. Clearly the inequality $\beta_2' \leq \beta_2^{(1)}$ holds if and only if $S - \sqrt{SD} \leq 0$ or equivalently

$$\frac{Ph_1 h_2}{\sqrt{1 + h_1^2 P + h_2^2 P}} \geq 1 \quad (126)$$

which is just Condition (37). Furthermore notice that $\beta_2^{(1)} < \frac{h_2}{h_1} P < \beta_2^{(2)}$ hence it remains to prove that $\beta_2^{(2)} \leq \beta_2''$ if and only if (37) holds. But this follows immediately by noticing that $\beta_2^{(2)} \leq \beta_2''$ can be rewritten as

$$2S^2 \leq h_1 h_2 P(S + \sqrt{SD}) \quad (127)$$

which is satisfied if and only if $S \leq D$, or equivalently Condition (37) holds.

APPENDIX C
THE DERIVATIONS IN THE PROOF OF THEOREM 5

In this section we give the derivation of the expressions of $\tilde{\mathbf{y}}_1$ in (102) and $\tilde{\mathbf{y}}_2$ in (104). To obtain $\tilde{\mathbf{y}}_1$, we process the channel output \mathbf{y} as

$$\begin{aligned} \tilde{\mathbf{y}}_1 &:= \alpha_1 \mathbf{y} - \sum_k a_k \beta_k \mathbf{d}_k \\ &= \underbrace{\sum_k (\alpha_1 - a_k \beta_k) \mathbf{x}_k}_{\tilde{\mathbf{z}}_1} + \alpha_1 \mathbf{z} + \alpha_1 \sum_k \mathbf{s}_k + \sum_k a_k \beta_k \mathbf{x}_k - \sum_k a_k \beta_k \mathbf{d}_k \end{aligned} \quad (128)$$

$$= \tilde{\mathbf{z}}_1 + \alpha_1 \sum_k \mathbf{s}_k + \sum_k a_k \beta_k (\mathbf{t}_k / \beta_k + \mathbf{d}_k - \gamma_k \mathbf{s}_k / \beta_k) \quad (129)$$

$$- \sum_k a_k \beta_k Q_{\Lambda_k^s / \beta_k}(\mathbf{t}_k / \beta_k + \mathbf{d}_k - \gamma_k \mathbf{s}_k / \beta_k) - \sum_k a_k \beta_k \mathbf{d}_k \quad (130)$$

$$= \tilde{\mathbf{z}}_1 + \sum_k a_k (\mathbf{t}_k - Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k - \alpha_1 \mathbf{s}_k)) + \sum_k (\alpha_1 - a_k \gamma_k) \mathbf{s}_k \quad (131)$$

$$= \tilde{\mathbf{z}}_1 + \sum_k a_k \tilde{\mathbf{t}}_k + \sum_k (\alpha_1 - a_k \gamma_k) \mathbf{s}_k \quad (132)$$

When the sum $\sum_k a_k \tilde{\mathbf{t}}_k$ is decoded, the term $\tilde{\mathbf{z}}_1 + \sum_k (\alpha_1 - a_k \gamma_k) \mathbf{s}_k$ which can be calculated using $\tilde{\mathbf{y}}_1$ and $\sum_k a_k \tilde{\mathbf{t}}_k$. For decoding the second sum we form the following with some numbers α_2' and λ :

$$\tilde{\mathbf{y}}_2 := \alpha_2' \mathbf{y} + \lambda \left(\tilde{\mathbf{z}}_1 + \sum_k (\alpha_1 - a_k \gamma_k) \mathbf{s}_k \right) - \sum_k b_k \beta_k \mathbf{d}_k \quad (133)$$

$$= \alpha_2' (h_1 \mathbf{x}_1 + h_2 \mathbf{x}_2 + \mathbf{s}_1 + \mathbf{s}_2 + \mathbf{z}) + \sum_k (\lambda \alpha_1 h_k - \lambda a_k \beta_k) \mathbf{x}_k + \lambda \alpha_1 \mathbf{z} + \lambda \sum_k (\alpha_1 - a_k \gamma_k) \mathbf{s}_k \quad (134)$$

$$= \sum_k (\alpha_2' + \lambda \alpha_1 - \lambda a_k \beta_k) \mathbf{x}_k + (\alpha_2' + \lambda \alpha_1) \mathbf{z} + \sum_k (\alpha_2' + \lambda \alpha_1 - \lambda a_k \gamma_k) \mathbf{s}_k - \sum_k b_k \beta_k \mathbf{d}_k \quad (135)$$

$$:= \sum_k (\alpha_2 - \lambda a_k \beta_k) \mathbf{x}_k + \alpha_2 \mathbf{z} + \sum_k (\alpha_2 - \lambda a_k \gamma_k) \mathbf{s}_k - b_k \beta_k \mathbf{d}_k \quad (136)$$

by defining $\alpha_2 := \alpha'_2 + \lambda\alpha_1$. In the same way as deriving $\tilde{\mathbf{y}}_1$, we can show

$$\begin{aligned}\tilde{\mathbf{y}}_2 &= \underbrace{\sum_k (\alpha_2 - \lambda a_k \beta_k - b_k \beta_k) \mathbf{x}_k + \alpha_2 \mathbf{z}}_{\tilde{\mathbf{z}}_2} + \sum_k (\alpha_2 - \lambda a_k \gamma_k) \mathbf{s}_k + \sum_k b_k \beta_k \mathbf{x}_k - \sum_k b_k \beta_k \mathbf{d}_k \\ &= \tilde{\mathbf{z}}_2 + \sum_k (\alpha_2 - a_k \gamma_k) \mathbf{s}_k + \sum_k b_k (\beta_k (\mathbf{t}_k / \beta_k + \mathbf{d}_k - \gamma_k \mathbf{s}_k / \beta_k) - \beta_k Q_{\Lambda_k^s / \beta_k}(\mathbf{t}_k / \beta_k + \mathbf{d}_k - \gamma_k \mathbf{s}_k / \beta_k)) - \sum_k b_k \beta_k \mathbf{d}_k \\ &= \tilde{\mathbf{z}}_2 + \sum_k (\alpha_2 - \lambda a_k \gamma_k - b_k \gamma_k) \mathbf{s}_k + \sum_k b_k \tilde{\mathbf{t}}_k\end{aligned}$$

by defining $\alpha_2 := \alpha'_2 + \lambda\alpha_1$ and $\tilde{\mathbf{z}}_2 := \sum_k (\alpha_2 - \lambda a_k \beta_k - b_k \beta_k) \mathbf{x}_k + \alpha_2 \mathbf{z}$.

ACKNOWLEDGMENT

The authors wish to thank Chien-Yi Wang, Bobak Nazer and Sung Hoon Lim for helpful comments.

REFERENCES

- [1] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, 2011.
- [2] M. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, 2010.
- [3] W. Nam, S.-Y. Chung, and Y. H. Lee, "Nested lattice codes for Gaussian relay networks with interference," *IEEE Trans. Inf. Theory*, vol. 57, 2011.
- [4] —, "Capacity of the Gaussian two-way relay channel to within 1/2 bit," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5488–5494, 2010.
- [5] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, "Integer-forcing linear receivers," arXiv e-print, Mar. 2010.
- [6] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2006.
- [7] B. Rimoldi and R. Urbanke, "A rate-splitting approach to the Gaussian multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 42, 1996.
- [8] O. Ordentlich, U. Erez, and B. Nazer, "Successive integer-forcing and its sum-rate optimality," in *Proceedings of the 51st Annual Allerton Conference on Communication, Control, and Computing*, 2013.
- [9] T. Philosof, R. Zamir, U. Erez, and A. Khisti, "Lattice strategies for the dirty multiple access channel," *IEEE Trans. Inf. Theory*, vol. 57, 2011.
- [10] R. Ahlswede, "Multi-way communication channels," in *Second International Symposium on Information Theory: Tsahkadsor, Armenia, USSR, Sept. 2-8, 1971*, 1973.
- [11] H. H.-J. Liao, "Multiple access channels." Ph.D. dissertation, Dept. Elec. Eng., Univ. of Hawai, Tech. Rep., 1972.
- [12] U. Erez and R. Zamir, "Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2293–2314, 2004.
- [13] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3401–3416, 2005.
- [14] V. Ntranos, V. Cadambe, B. Nazer, and G. Caire, "Asymmetric compute-and-forward," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct. 2013, pp. 1174–1181.
- [15] O. Ordentlich and U. Erez, "Precoded integer-forcing universally achieves the MIMO capacity to within a constant gap," arXiv e-print, Jan. 2013.
- [16] J. Zhu and M. Gastpar, "Asymmetric compute-and-forward with CSIT," in *International Zurich Seminar on Communications*, 2014.
- [17] B. Nazer, "Successive compute-and-forward," in *International Zurich Seminar on Communications*, 2012, p. 103.
- [18] A. Somekh-Baruch, S. Shamai, and S. Verdú, "Cooperative multiple-access encoding with states available at one transmitter," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4448–4469, Oct. 2008.
- [19] S. Kotagiri and J. Laneman, "Multiaccess channels with state known to some encoders and independent messages," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, no. 1, Mar. 2008.
- [20] I.-H. Wang, "Approximate capacity of the dirty multiple-access channel with partial state information at the encoders," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2781–2787, May 2012.
- [21] M. H. M. Costa, "Writing on dirty paper (corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.
- [22] S. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Problemy Pered. Inf. (Probl. Inf. Trans.)*, vol. 9, 1980.
- [23] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, 2002.